μΠλ∀

Κρυπτοσυστηματα πακετου: απο το DES στο AES

Χρήστος Καπούτσης

μΠλ∀

Κρυπτοσυστηματα πακετου: απο το DES στο AES

Χρήστος Καπούτσης

Αύγουστος 2000

Πρόλογος

Το θέμα αυτής της εργασίας είναι τα κρυπτοσυστήματα πακέτου, μια από τις δύο βασικές κατηγορίες συμμετρικών κρυπτοσυστημάτων που χρησιμοποιούνται σήμερα. Μεγάλο μέρος της μελέτης αυτών των συστημάτων έχει γίνει πάνω στο DES (Data Encryption Standard), το κυβερνητικό πρότυπο των ΗΠΑ για την κρυπτογράφηση ευαίσθητων δεδομένων, που έχει ορισθεί ήδη από το 1977. Για λόγους που θα συζητήσουμε, το DES πρόκειται να αντικατασταθεί μέσα στον επόμενο χρόνο από ένα νέο πρότυπο, με το όνομα AES (Advanced Encryption Standard).

Στο Κεφάλαιο 1 συζητάμε τις βασικές έννοιες και εισάγουμε τους απαραίτητους συμβολισμούς. Το Κεφάλαιο 2 περιγράφει το DES και τους τυποποιημένους τρόπους λειτουργίας του. Στο Κεφάλαιο 3 κατηγοριοποιούμε τις επιθέσεις που μπορεί να δεχθεί ένα κρυπτοσύστημα και δίνουμε δύο ορισμούς για το πότε αυτό μπορεί να θεωρηθεί ασφαλές. Τα Κεφάλαια 4 και 5 εξηγούν τη βασική ιδέα πίσω από τις δύο πιο γνωστές μη τετριμμένες επιθέσεις που εφαρμόζονται στα κρυπτοσυστήματα πακέτου. Τέλος, στο 6ο Κεφάλαιο περιγράφουμε ένα από τα κρυπτοσυστήματα πακέτου που είναι υποψήφια για να αποτελέσουν το AES, αυτό που φαίνεται να είναι το επικρατέστερο.

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

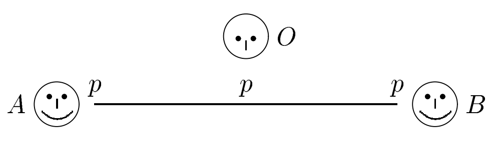
1. Βασικές έννοιες

1.1. Το πρόβλημα. Ένα από τα προβλήματα που καλείται να λύσει η σύγχρονη κρυπτογραφία (και το οποίο είναι και το ιδρυτικό του κλάδου) είναι η διαφύλαξη της ασφάλειας της επικοινωνίας δύο μερών (Σχήμα 1): Ο *πομπός* A θέλει να μεταδώσει στο *δέκτη* B ένα μήνυμα p διαμέσου κάποιου καναλιού. Αλλά ο *εχθρός* O έχει και αυτός πρόσβαση στο κανάλι, κι έτσι μπορεί να υποκλέψει το p και να το επεξεργαστεί με οποιονδήποτε τρόπο επιθυμεί. Ψάχνουμε μεθόδους για να δυσχεράνουμε την προσπάθεια του εχθρού.

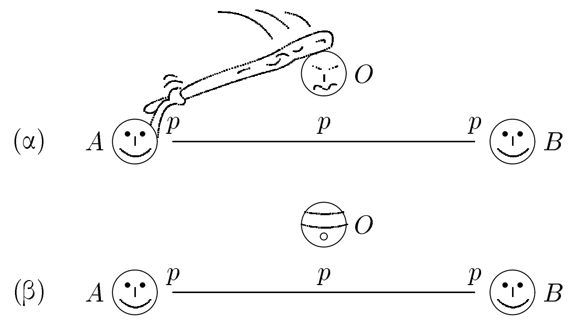
Τα διάφορα στιγμιότυπα αυτού του προβλήματος είναι πραγματικά παρά πολλά. Ο πομπός, ο δέκτης, το μήνυμα, το κανάλι, ο εχθρός είναι απλώς ρόλοι, που σε διαφορετικές περιστάσεις μπορούν να παιχτούν από διαφορετικές οντότητες. Στην πιο απλή περίπτωση, ο πομπός και ο δέκτης είναι αντίστοιχα ο Ερωτόκριτος και η Αρετούσα, ο εχθρός είναι ο πατέρας της δεύτερης και το κανάλι η τροφός της, ενώ το μήνυμα είναι πιθανότατα κάποια αρχαιοελληνική εκδοχή του «σ' αγαπώ». Σε ένα πιο σύγχρονο και λιγότερο ρομαντικό στιγμιότυπο, ο πομπός είναι ένας συνδεδεμένος στο Διαδίκτυο υπολογιστής, ο δέκτης ένας επικοινωνιακός δορυφόρος, ο εχθρός ένας αγουροξυπνημένος υπάλληλος του Echelon, το μήνυμα κάτι σαν 00110101 και το κανάλι ο τρισδιάστατος χώρος.

Το πρόβλημα είναι αρκετά γενικό ώστε να περιλαμβάνει και στιγμιότυπα στα οποία η ίδια οντότητα παίζει περισσότερους από έναν ρόλους. Για παράδειγμα, κατά τη μετάδοση ενός μηνύματος μέσω κάποιου αγγελιοφόρου, ο τελευταίος είναι ταυτόχρονα και το κανάλι αλλά και ο εχθρός της επικοινωνίας. Παρόμοια, όταν κανείς αποθηκεύει ένα αρχείο στον υπολογιστή του με σκοπό να το ανακτήσει αργότερα, τότε συμμετέχει σε μια επικοινωνία στην οποία είναι ταυτόχρονα και πομπός και δέκτης.

Προτού ακόμη επινοηθεί η λέξη «κρυπτογραφία», η λύση που προτάθηκε για το πρόβλημα ήταν αυτή του Σχήματος 2(α). Όμως αυτό λέγεται ...πόλεμος και δεν τον ακολουθούμε εδώ. Μια άλλη λύση (Σχήμα 2(β)), περισσότερο έξυπνη και λιγότερο βάρβαρη, είναι να παραπλανήσουμε τον εχθρό, ώστε αυτός να μην αντιληφθεί καν ότι



Σχημα 1. Το βασικό πρόβλημα: ο πομπός A στέλνει στο δέκτη B το μήνυμα p, αλλά ο εχθρός O μπορεί στην πορεία να το υποκλέψει.



Σχημα 2. Πόλεμος και στεγανογραφία: δυο λύσεις που δεν ακολουθούμε.

πραγματοποιείται η επικοινωνία.[1] Αυτή την τεχνική την ονομάζουμε *στεγανογραφία* (steganography)· επίσης δεν μας απασχολεί εδώ.

Δεχόμαστε λοιπόν ότι ο εχθρός (είναι υγιής και) μπορεί να αντιληφθεί τη μετάδοση του μηνύματος, μπορεί να το υποκλέψει και μπορεί ακολούθως να το επεξεργαστεί με οποιονδήποτε τρόπο. Στο πλαίσιο αυτό, η καλύτερη ιδέα μοιάζει να είναι η εξής (Σχήμα 3): Ανάμεσα σ' αυτόν και στο κανάλι, καθένας από τους πομπό και δέκτη τοποθετεί ένα «κουτί». Το κουτί του πομπού υπολογίζει κάποιον αντιστρέψιμο μετασχηματισμό

$$e : \mathcal{P} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathcal{Q}$$

από το χώρο $\mathcal{P}$ όλων των δυνατών μηνυμάτων σε κάποιον νέο χώρο $\mathcal{Q}$ των μετασχηματισμένων μηνυμάτων, ενώ το κουτί του δέκτη, που δέχεται την είσοδό του από το κανάλι, υπολογίζει τον αντίστροφο μετασχηματισμό $d = e^{-1}$ του e. Για να μεταδώσει το p, ο πομπός το αφήνει στην είσοδο του κουτιού του. Το μετασχηματισμένο μήνυμα $q = e(p)$ διασχίζει το κανάλι μέχρι την είσοδο του κουτιού του δέκτη, ο οποίος και παραλαμβάνει το αρχικό μήνυμα

$$d(q) = e^{-1}\big(e(p)\big) = p.$$

Στο ενδιάμεσο, ο εχθρός μπορεί να κλέψει το μετασχηματισμένο μήνυμα q, αλλά δεν μπορεί να υπολογίσει το αρχικό μήνυμα p, αν δεν ξέρει τον αντίστροφο μετασχηματισμό d.

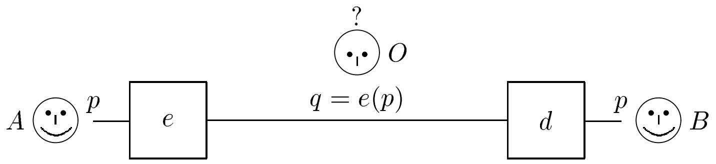
Για παράδειγμα, αν ο χώρος $\mathcal{P}$ είναι το σύνολο όλων των μικρών γραμμάτων του λατινικού αλφαβήτου, τότε ένας πιθανός μετασχηματισμός e είναι αυτός που περιγράφεται από τον κανόνα του Καίσαρα:[2]

[1]Για παράδειγμα, ο πομπός γράφει το μήνυμα πάνω σε λευκό χαρτί και με μια ειδική μελάνη, που γίνεται ορατή μόνο όταν το χαρτί τοποθετηθεί μπροστά σε μια πηγή φωτός. Όποιος δεν έχει υποπτευθεί τι συμβαίνει νομίζει ότι το χαρτί είναι άγραφο. Όμως ο ειδοποιημένος δέκτης μπορεί να διαβάσει το αόρατο κείμενο.

Ένα ακόμη πιο εντυπωσιακό παράδειγμα είναι το εξής: ο πομπός γράφει το μήνυμα στο ξυρισμένο κεφάλι ενός αγγελιοφόρου (το κανάλι της συγκεκριμένης επικοινωνίας) και αυτός ξεκινάει για τον δέκτη μόνο αφού ξαναμεγαλώσουν τα μαλλιά του. Κατά τη διάρκεια του ταξιδιού κανένας σωματικός έλεγχος πάνω του δεν μπορεί να αποκαλύψει το μήνυμα. Αλλά ο δέκτης μπορεί να το διαβάσει εύκολα, ξαναξυρίζοντας τον αγγελιοφόρο. Είναι ενδιαφέρον το ότι με τη συγκεκριμένη τεχνική το μήνυμα προστατεύεται κι από αυτόν ακόμη τον αγγελιοφόρο!

Υπάρχουν πολλές τέτοιες παλιές [**14**], αλλά και νεότερες [**12, 13**] εφαρμογές της ίδιας γενικής ιδέας.

[2]Πρόκειται για τον κρυπτογραφικό κανόνα που χρησιμοποιούσε ο Ιούλιος Καίσαρας.



ΣΧΗΜΑ 3

> «αντικατάστησε κάθε γράμμα με το γράμμα που βρίσκεται τρεις θέσεις μετά από αυτό στο αλφάβητο».

δηλαδή από τον πίνακα

p	a	b	c	d	e	f	g	...	t	u	v	w	x	y	z
$e(p)$	d	e	f	g	h	i	j	...	w	x	y	z	a	b	c

Τότε ο χώρος $\mathcal{Q}$ των μετασχηματισμένων μηνυμάτων είναι βεβαίως ο ίδιος ο $\mathcal{P}$ και ο αντίστροφος μετασχηματισμός d είναι ο προφανής. Έτσι η ακολουθία των παρακάτω έξι μηνυμάτων

a t t a c k

μετασχηματίζεται στην

d w w d f n

και ο ανυποψίαστος για τον d εχθρός δεν προλαβαίνει να προετοιμαστεί.

Προφανώς, η λύση του Σχήματος 3 βασίζεται στη μυστικότητα του d (που στη συγκεκριμένη περίπτωση ισοδυναμεί με τη μυστικότητα του e). Κι αυτό σε αρκετές περιπτώσεις δεν είναι καθόλου δύσκολο να εξασφαλιστεί. Αν, για παράδειγμα, τα δυο κουτιά είναι απλοί κανόνες (σαν αυτόν του Καίσαρα) που ο Ερωτόκριτος και η Αρετούσα μπορούν εύκολα να απομνημονεύσουν και να εκτελούν, τότε αρκεί κανείς από τους δύο να μην μαρτυρήσει αυτούς τους κανόνες στον αχώνευτο βασιλιά Ηρακλή. Υπάρχουν όμως και πολλές περιπτώσεις στις οποίες η μυστικότητα του d δεν είναι εύκολο να διατηρηθεί: αν ο πομπός είναι τα κεντρικά γραφεία της Coca-Cola στην Atlanta, ο δέκτης είναι το τυχόν υποκατάστημα της επιχείρησης ανά τον κόσμο και το κουτί του δέκτη είναι ένας αλγόριθμος υλοποιημένος σε μια κάρτα επέκτασης στον κεντρικό υπολογιστή του καταστήματος, τότε υπάρχουν πάρα πολλά τέτοια κουτιά για να μπορεί κάποιος να υποθέσει ότι θα είναι όλα ασφαλή και (πολύ περισσότερο) για να μπορεί να τα αντικαθιστά όλα κάθε φορά που η Pepsi Cola θα κλέβει ένα από αυτά.

1.2. Συμμετρική κρυπτογραφία. Η λύση λοιπόν δεν είναι αρκετά ευέλικτη, και μια βελτίωση φαίνεται στο Σχήμα 4: Το κουτί του πομπού υλοποιεί τώρα μια ολόκληρη οικογένεια μετασχηματισμών

$$\mathcal{E} = \{e_k \mid k \in \mathcal{K}\},$$

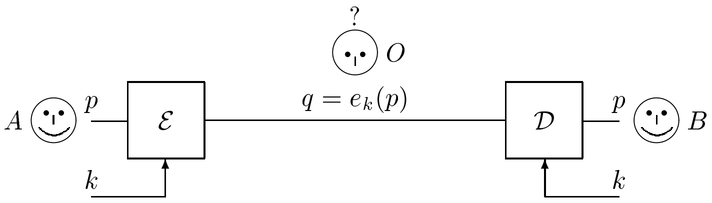
όπου $\mathcal{K}$ είναι ένα σύνολο δεικτών ή *κλειδιών* (keys) και, για κάθε $k \in \mathcal{K}$,

$$e_k : \mathcal{P} \rightarrowtail\!\!\!\!\rightarrow \mathcal{Q}.$$

Αντίστοιχα, το κουτί του δέκτη υλοποιεί την οικογένεια των αντίστροφων μετασχηματισμών

$$\mathcal{D} = \{d_k \mid k \in \mathcal{K}\}, \qquad \text{με} \quad d_k = e_k^{-1} : \mathcal{Q} \rightarrowtail\!\!\!\!\rightarrow \mathcal{P}.$$

Έχοντας προσυμφωνήσει ένα κοινό κλειδί $k \in \mathcal{K}$, πομπός και δέκτης τροφοδοτούν τα κουτιά τους με αυτό, ώστε να επιλέξουν τους μετασχηματισμούς e_k και d_k αντίστοιχα



Σχημα 4

από τις δύο οικογένειες $\mathcal{E}$ και $\mathcal{D}$. Το υπόλοιπο της επικοινωνίας γίνεται όπως και πριν.

Ένα εύκολο παράδειγμα προκύπτει από μια γενίκευση της ιδέας του Καίσαρα από την προηγούμενη ενότητα: αντί να αντικαθιστά κάθε γράμμα με το τρίτο επόμενό του μέσα στο αλφάβητο, ο πομπός μπορεί να το αντικαθιστά με το k-οστό επόμενό του, για κάποιο $k \in \{1, 2, \ldots, 25\}$ που έχει προσυμφωνηθεί ανάμεσα σ' αυτόν και στο δέκτη. Οπότε η ακολουθία των μετασχηματισμένων μηνυμάτων

d w w d f n

αντιστοιχεί στην ακολουθία

a t t a c k

αν $k = 3$, αλλά στην ακατανόητη

b u u b d l

αν $k = 2$. Βεβαίως, στη συγκεκριμένη περίπτωση ο χώρος των κλειδιών είναι ο $\mathcal{K} = \{1, 2, \ldots, 25\}$ και για κάθε $k \in \mathcal{K}$ οι μετασχηματισμοί e_k, d_k οι προφανείς.

Ακόμη κι αν μπορέσει να κλέψει το κουτί του δέκτη, ο εχθρός δεν μπορεί να βρει άμεσα το αρχικό μήνυμα, γιατί δεν ξέρει το συμφωνημένο κλειδί k κι έτσι δεν μπορεί να διαλέξει το σωστό αντίστροφο μετασχηματισμό d_k. Το να δοκιμάσει όλες τις πιθανές τιμές του κλειδιού μπορεί να γίνει απαγορευτικά χρονοβόρο, αν το σύνολο $\mathcal{K}$ έχει επιλεγεί ανάλογα μεγάλο.[3] Αλλά ακόμη κι αν ο εχθρός καταφέρει τελικά με κάποιον τρόπο να βρει το κλειδί, ο πομπός και ο δέκτης (εφόσον αντιληφθούν τη διαρροή) μπορούν να συνεχίσουν να επικοινωνούν χρησιμοποιώντας τα ίδια κουτιά και αλλάζοντας μόνο το κλειδί.

Από νωρίς, η ιδέα της προσθήκης του κλειδιού φάνηκε ότι είναι τόσο πετυχημένη που ακύρωσε εντελώς την ανάγκη να διατηρείται μυστικό το κουτί του δέκτη (Kerckhoffs [**14**]). Με άλλα λόγια, δεχόμαστε εξαρχής ότι ο εχθρός ξέρει την οικογένεια μετασχηματισμών $\mathcal{D}$, δηλαδή το πώς από ένα κλειδί k και ένα μετασχηματισμένο μήνυμα q (που έχει υποκλέψει) να υπολογίζει το μήνυμα $p = d_k(q)$, και ο μόνος λόγος που δεν μπορεί να το κάνει είναι το ότι δεν ξέρει το κλειδί. Δεχόμαστε επίσης ότι ο εχθρός ξέρει και το κουτί του πομπού, δηλαδή την οικογένεια μετασχηματισμών $\mathcal{E}$.

Βεβαίως, οι παραδοχές αυτές δεν είναι πάντα απαραίτητο να ισχύουν. Και είναι σίγουρο ότι η μυστικότητα των $\mathcal{E}$, $\mathcal{D}$ αυξάνει την ασφάλεια της επικοινωνίας. Υπάρχουν ωστόσο και περιπτώσεις που εκ των πραγμάτων οι $\mathcal{E}$, $\mathcal{D}$ πρέπει να είναι δημόσια γνωστές: π.χ., δεν μπορεί να γίνει διαφορετικά αν θέλουμε να εκμεταλλευτούμε τις ευκολίες που προσφέρει η ευρείας κλίμακας τυποποίηση της επικοινωνίας αυτού του είδους.

[3] Στο παραπάνω παράδειγμα, το $|\mathcal{K}|$ είναι μόνο 25 και δεν υπάρχει ουσιαστικό πρόβλημα για τον εχθρό· όμως τα πράγματα δυσκολεύουν στην περίπτωση που οι A και B είναι Κινέζοι ...

Η γενική ιδέα της λύσης του Σχήματος 4 χρησιμοποιείται σήμερα ευρύτατα και αναφέρεται ως *κρυπτογραφία ιδιωτικού κλειδιού* (private key cryptography) ή *κρυπτογραφία ενός κλειδιού* (one-key cryptography) ή *συμμετρική κρυπτογραφία* (symmetric cryptography). Τα ονόματα προκύπτουν από την βασική απαίτηση ότι ένα κοινό κλειδί πρέπει να έχει προσυμφωνηθεί ανάμεσα στον πομπό και το δέκτη πριν αρχίσει η επικοινωνία τους διαμέσου του ανασφαλούς καναλιού. Αυτό δεν είναι πάντα απλό να γίνει και τότε αναδεικνύεται ως ένα πολύ σοβαρό μειονέκτημα της μεθόδου.

Πράγματι, για να συμφωνήσουν στο κοινό κλειδί, ο πομπός και ο δέκτης πρέπει με κάποιον τρόπο να επικοινωνήσουν πριν αρχίσει η κυρίως επικοινωνία τους, για την ασφάλεια της οποίας γίνεται όλη η συζήτηση. Οπωσδήποτε, για αυτήν την προκαταρκτική επικοινωνία δεν μπορούν να χρησιμοποιήσουν το ανασφαλές κανάλι που πρόκειται να χρησιμοποιήσουν στην κυρίως επικοινωνία, γιατί έτσι ο εχθρός θα μάθει κι αυτός το κλειδί. Επομένως, θα πρέπει να χρησιμοποιήσουν ένα ασφαλές κανάλι, στο οποίο ο εχθρός να μην έχει πρόσβαση.

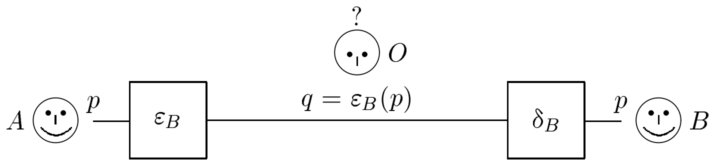
Αυτή η απαίτηση για την ύπαρξη ενός ασφαλούς καναλιού φαίνεται εκ πρώτης όψεως να ακυρώνει όλη την κουβέντα: αν όντως υπάρχει ασφαλές κανάλι, τότε γιατί ο πομπός και ο δέκτης δεν χρησιμοποιούν κατευθείαν αυτό για την κυρίως επικοινωνία τους, να τελειώνουμε; Η απάντηση είναι ότι σε πολλές περιπτώσεις το ασφαλές κανάλι, που όντως υπάρχει και μπορεί να χρησιμοποιηθεί για την επιλογή του κλειδιού, δεν μπορεί να χρησιμοποιηθεί για την κυρίως επικοινωνία. Παραδείγματος χάριν, δύο πράκτορες της CIA στην Ελλάδα μπορούν εύκολα να συμφωνούν ένα νέο κλειδί κάθε φορά που συναντώνται στο υπουργικό συμβούλιο, ενώ η κυρίως επικοινωνία τους μπορεί να γίνεται μέσω του Διαδικτύου και με βάση το πιο πρόσφατα συμφωνημένο κλειδί. Μια άλλη περίπτωση είναι αυτή κατά την οποία το κλειδί μπορεί να αποσταλεί από τον πομπό στο δέκτη μέσω της DHL και στη συνέχεια η κυρίως επικοινωνία, που περιλαμβάνει μερικές χιλιάδες σελίδες απόρρητου υλικού, μπορεί να γίνει μέσω των ΕΛΤΑ και με το φθηνότερο δυνατό τιμολόγιο.

1.3. Ασύμμετρη κρυπτογραφία. Σε κάθε περίπτωση λοιπόν, η συμμετρική κρυπτογραφία προϋποθέτει μια σύντομη προκαταρκτική επικοινωνία ανάμεσα στον πομπό και το δέκτη για την επιλογή του κλειδιού διαμέσου ενός ασφαλούς καναλιού. Και, παρόλο που στις περισσότερες περιπτώσεις υπάρχει, αυτό το ασφαλές κανάλι δεν είναι τόσο φθηνό, ταχύ και ευέλικτο όσο το ανασφαλές κανάλι της κύριας επικοινωνίας. Οπότε, το εύλογο ερώτημα είναι αν υπάρχει κάποια τεχνική που να επιτρέπει τη χρήση του ανασφαλούς καναλιού της κύριας επικοινωνίας ακόμη και για την επιλογή του κλειδιού.

Η απάντηση είναι θετική και έχει δοθεί με τα *συστήματα διανομής δημόσιου κλειδιού* (public key distribution systems) [**18, 7**] (αλλά και [**9, 36**]). Όμως η ιδέα αυτής της απάντησης περιέχει κάτι ακόμη καλύτερο: την *κρυπτογραφία δημόσιου κλειδιού* (public key cryptography) ή *κρυπτογραφία δύο κλειδιών* (two-key cryptography) ή *ασύμμετρη κρυπτογραφία* (asymmetric cryptography) [**18, 7**] (αλλά και [**9, 8**]), με την οποία ακυρώνεται αυτή καθεαυτήν η ανάγκη της ύπαρξης κάποιου κοινού μυστικού κλειδιού ανάμεσα στον πομπό και το δέκτη.

Η τεχνική φαίνεται στο Σχήμα 5. Καθένας B που θέλει να μπορεί να δέχεται κρυπτογραφημένα μηνύματα επιλέγει δύο συναρτήσεις,

- μια συνάρτηση (κρυπτογράφησης) $\varepsilon_B : \mathcal{P} \to \mathcal{Q}$, την οποία και δημοσιεύει, ώστε να γίνει γνωστή σε κάθε πιθανό πομπό μηνύματος προς αυτόν, και



Σχημα 5

- μια συνάρτηση (αποκρυπτογράφησης) $\delta_B : \mathcal{Q} \to \mathcal{P}$, την οποία κρατάει μυστική,

με τρόπο ώστε να ικανοποιούνται τρεις πολύ σημαντικές συνθήκες:

1. οι ε_B, δ_B να είναι εύκολα υπολογίσιμες,
2. για κάθε $p \in \mathcal{P}$ να ισχύει ότι $\delta_B\big(\varepsilon_B(p)\big) = p$, δηλαδή για κάθε $q \in \varepsilon_B[\mathcal{P}]$ η δ_B επιστρέφει μια λύση της εξίσωσης
$$\varepsilon_B(p) = q,$$
3. ο εχθρός να μην έχει αποτελεσματικό γενικό τρόπο να λύνει αυτήν την εξίσωση όσο δεν γνωρίζει την δ_B, παρόλο που γνωρίζει την ε_B.

Τότε, οποιοσδήποτε θέλει να στείλει κάποιο μήνυμα $p \in \mathcal{P}$ στο δέκτη B, απλώς βρίσκει τη συνάρτηση ε_B (στο χώρο που την έχει δημοσιεύσει ο B), υπολογίζει εύκολα την τιμή $q = \varepsilon_B(p)$ (συνθήκη 1), και τη στέλνει στο B. Εκείνος υπολογίζει εύκολα την τιμή $\delta_B(q)$ (συνθήκη 1), που είναι ακριβώς το αρχικό μήνυμα,
$$\delta_B(q) = \delta_B\big(\varepsilon_B(p)\big) = p \qquad \text{(συνθήκη 2)}.$$
Από τη μεριά του, ο εχθρός δεν μπορεί από την μεταδοθείσαι τιμή q να υπολογίσει το p (συνθήκη 3). Και η μυστική συνάρτηση δ_B είναι απόλυτα ασφαλής, γιατί δεν χρειάζεται ποτέ να μεταδοθεί.

Ζευγάρια συναρτήσεων (ε, δ) που έχουν τις συγκεκριμένες τρεις ιδιότητες (αλλά και άλλες, που τα καθιστούν ακόμη πιο χρήσιμα) έχουν βρεθεί [**27**] (αλλά και [**9, 5, 35**]), κι έτσι η τεχνική της συμμετρικής κρυπτογραφίας είναι πρακτικά εφαρμόσιμη.

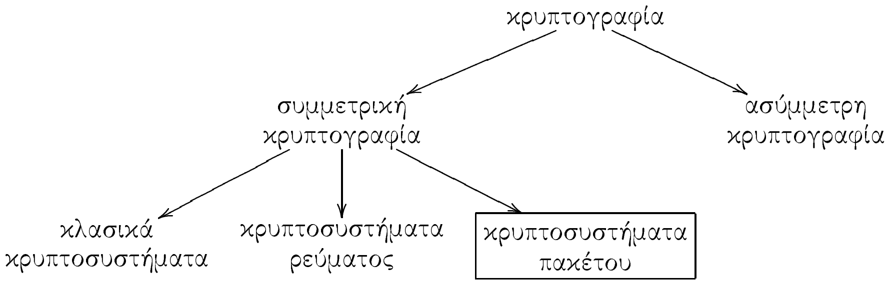
Το βασικό της μειονέκτημα είναι ο χρόνος που απαιτείται για τον υπολογισμό των συναρτήσεων ε και δ. Παρόλο που, στα πιο πρακτικά από τα υπάρχοντα ασύμμετρα συστήματα αυτός ο χρόνος είναι αρκετά μικρός ώστε να καθιστά το σύστημα εξαιρετικά πρακτικό, εξακολουθεί να είναι σημαντικά μεγαλύτερος από το χρόνο που απαιτούν οι αντίστοιχοι μετασχηματισμοί e_k και d_k των πιο συνηθισμένων συμμετρικών συστημάτων.[4]

2. Κρυπτοσυστήματα πακέτου

Τα πράγματα γίνονται λίγο πιο συγκεκριμένα με τον παρακάτω ορισμό [**34**, §1.1].

2.1. Ορισμος. Λέμε *κρυπτοσύστημα* (cryptosystem, cipher) κάθε πεντάδα της μορφής $(\mathcal{P}, \mathcal{Q}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, όπου τα $\mathcal{P}$, $\mathcal{Q}$, $\mathcal{K}$ είναι πεπερασμένα σύνολα και τα $\mathcal{E}$, $\mathcal{D}$ είναι οικογένειες συναρτήσεων
$$\mathcal{E} = \{e_k \mid k \in \mathcal{K}\} \quad \text{και} \quad \mathcal{D} = \{d_k \mid k \in \mathcal{K}\}$$

[4] Για παράδειγμα, αναφέρεται [**34**, p. 128] ότι μια από τις πιο γρήγορες υλοποιήσεις του (ασύμμετρου συστήματος) RSA είναι 1500 φορές πιο αργή από μια αντίστοιχα αποτελεσματική υλοποίηση του (συμμετρικού συστήματος) DES.



Σχημα 6. Βρισκόμαστε στην γενικότερη περιοχή της συμμετρικής κρυπτογραφίας και ασχολούμαστε με τα κρυπτοσυστήματα πακέτου.

τέτοιες ώστε, για κάθε $k \in \mathcal{K}$:

$$e_k : \mathcal{P} \to \mathcal{Q} \quad \text{και} \quad d_k : \mathcal{Q} \to \mathcal{P}$$

και επίσης

$$\text{για κάθε } p \in P : \quad d_k\big(e_k(p)\big) = p. \tag{1}$$

Το νόημα είναι ότι το σύνολο $\mathcal{P}$ περιέχει όλα τα στοιχειώδη (ως προς την κρυπτογράφηση που επιχειρεί το συγκεκριμένο κρυπτοσύστημα) κομμάτια από τα οποία μπορεί να αποτελείται ένα μήνυμα. Κάθε τέτοιο κομμάτι το λέμε *κείμενο* (plaintext). Αντίστοιχα, το $\mathcal{Q}$ περιέχει τις τιμές που παράγονται κατά το μετασχηματισμό των κειμένων. Ονομάζουμε κάθε τέτοια τιμή *κρυπτοκείμενο* (ciphertext). Και τέλος, το $\mathcal{K}$ περιέχει κάθε τιμή που μπορεί να χρησιμοποιηθεί ως *κλειδί* (key). Στο παράδειγμα της Ενότητας 1.2 τόσο τα κείμενα όσο και τα κρυπτοκείμενα είναι μικρά γράμματα του λατινικού αλφαβήτου, ενώ τα κλειδιά είναι οι τιμές από το 1 ως το 25.

2.2. Παρατηρηση. Είναι άμεσο από την Εξίσωση (1) ότι η συνάρτηση e_k είναι μονομορφισμός, για κάθε $k \in \mathcal{K}$. Επομένως $|\mathcal{P}| \leq |\mathcal{Q}|$.

Στην ειδική περίπτωση που τα $\mathcal{P}$ και $\mathcal{Q}$ είναι ισοπληθικά, η αρχή του περιστερεώνα συνεπάγεται ότι η e_k είναι και επιμορφισμός. Άρα είναι αντιστοιχία και επομένως η d_k είναι η αντίστροφή της, δηλαδή $d_k = e_k^{-1}$, για κάθε $k \in \mathcal{K}$.

Τα κρυπτοσυστήματα που πρόκειται να εξετάσουμε σ' αυτήν την εργασία είναι όλα *κρυπτοσυστήματα πακέτου* (block ciphers). Αυτή είναι μόνο η μία από τις δύο κατηγορίες σύγχρονων κρυπτοσυστημάτων που εφαρμόζουν την τεχνική της συμμετρικής κρυπτογραφίας. Η άλλη κατηγορία είναι αυτή των *κρυπτοσυστημάτων ρεύματος* (stream ciphers) [**31**] και δεν πρόκειται να μας απασχολήσει. Βεβαίως, συμμετρικά είναι και όλα τα κλασικά κρυπτοσυστήματα [**34**, §1.1] που επίσης δεν εξετάζουμε εδώ. (Σχήμα 6.)

Στα κρυπτοσυστήματα πακέτου δεχόμαστε από την αρχή ότι κάθε μήνυμα είναι μια πεπερασμένη ακολουθία δυαδικών ψηφίων. Η ακολουθία αυτή χωρίζεται σε διαδοχικά *πακέτα* (blocks) των n ψηφίων, όπου n μια σταθερά (παράμετρος του κρυπτοσυστήματος), τα οποία και κρυπτογραφούνται διαδοχικά και ανεξάρτητα το ένα από το άλλο. Η κρυπτογράφηση ενός πακέτου παράγει ένα άλλο πακέτο, επίσης n ψηφίων, και το κρυπτογραφημένο μήνυμα είναι η παράθεση των κρυπτογραφημένων πακέτων με την προφανή σειρά. Στην ειδική περίπτωση που το μήκος ενός μηνύματος δεν είναι πολλαπλάσιο του n, κατάλληλο πλήθος ψηφίων επιτίθεται σ' αυτό σύμφωνα με κάποια προεπιλεγμένη σύμβαση.

Για παράδειγμα, έστω ότι $n = 8$ και ότι το μήνυμα είναι η ακολουθία των $N = 37$ ψηφίων

$$1000000010011111100111101010010010011.$$

Για να κάνουμε το μήκος πολλαπλάσιο του n, επιθέτουμε στο μήνυμα 3 επιπλέον (μηδενικά) ψηφία, ώστε $N' = 40$, και χωρίζουμε το αποτέλεσμα σε πακέτα:

$$10000000 \quad 10011111 \quad 10011110 \quad 10100100 \quad 10011000.$$

Ακολούθως, κρυπτογραφούμε κάθε πακέτο χωριστά και ανεξάρτητα από τα υπόλοιπα, παράγοντας πέντε νέα πακέτα, π.χ. τα

$$01001100 \quad 01101111 \quad 01110110 \quad 01100101 \quad 01010101$$

ώστε το κρυπτογραφημένο μήνυμα είναι η ακολουθία

$$0100110001101111011101100110010101010101.$$

Επομένως, τα κείμενα ενός τέτοιου κρυπτοσυστήματος είναι όλες οι n-ψήφιες δυαδικές ακολουθίες. Δηλαδή $\mathcal{P} = \mathbb{B}^n$, όπου $\mathbb{B} = \{0, 1\}$ το δυαδικό αλφάβητο. Τα δε κρυπτοκείμενα είναι επίσης τέτοιες ακολουθίες, οπότε $\mathcal{Q} \subseteq \mathbb{B}^n$. Όμως από την Παρατήρηση 2.2 ξέρουμε ότι $|\mathcal{P}| \leq |\mathcal{Q}|$, οπότε πρέπει να είναι $\mathcal{Q} = \mathbb{B}^n$.

Δεχόμαστε επίσης σε ένα κρυπτοσύστημα πακέτου ότι τα κλειδιά είναι κι αυτά δυαδικές ακολουθίες, σταθερού μήκους m, για κάποιο m (μια δεύτερη παράμετρο του κρυπτοσυστήματος). Δηλαδή $\mathcal{K} = \mathbb{B}^m$.

2.3. Ορισμος. Έστω $n, m \geq 1$. Λέμε *κρυπτοσύστημα πακέτου* (block cipher) με διαστάσεις $n \times m$ κάθε κρυπτοσύστημα $(\mathcal{P}, \mathcal{Q}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ στο οποίο $\mathcal{P} = \mathcal{Q} = \mathbb{B}^n$ και $\mathcal{K} = \mathbb{B}^m$.

Από την Παρατήρηση 2.2, έπεται ότι για κάθε $k \in \mathcal{K}$ η συνάρτηση e_k είναι μια αντιστοιχία του $\mathcal{P} = \mathbb{B}^n$ στο $\mathcal{Q} = \mathbb{B}^n$, δηλαδή μια μετάθεση του $\mathbb{B}^n$. Και η d_k είναι ακριβώς η αντίστροφη μετάθεση. Επομένως, το $\mathcal{E}$ δεν είναι τίποτα περισσότερο από μια πεπερασμένη ακολουθία 2^m μεταθέσεων του $\mathbb{B}^n$. Και ορίζει πλήρως το κρυπτοσύστημα, αφού τότε το $\mathcal{D}$ είναι απλώς η ισομήκης ακολουθία των αντίστροφων μεταθέσεων.

2.4. Προταση. *Υπάρχει μια αντιστοιχία ανάμεσα στο σύνολο όλων των κρυπτοσυστημάτων πακέτου με διαστάσεις $n \times m$ και στο σύνολο όλων των μήκους 2^m ακολουθιών μεταθέσεων του $\mathbb{B}^n$.*

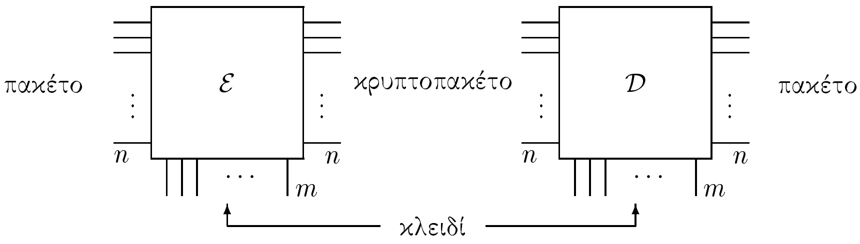
Αποδειξη. Η συνάρτηση που για κάθε κρυπτοσύστημα πακέτου $(\mathcal{P}, \mathcal{Q}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ επιστρέφει το $\mathcal{E}$ είναι αυτή η αντιστοιχία. ⊣

2.5. Πορισμα. *Το πλήθος των διαφορετικών κρυπτοσυστημάτων πακέτου με διαστάσεις $n \times m$ είναι*

$$(2^n!)^{2^m}.$$

3. Κατασκευή

Παρόλο που η συνολοθεωρητική περιγραφή της προηγούμενης ενότητας μάλλον δεν το έχει κάνει σαφές, το να φτιάξει κανείς ένα κρυπτοσύστημα πακέτου με διαστάσεις $n \times m$ είναι κάτι μόνο λίγο περισσότερο από το να φτιάξει δύο «κουτιά», $\mathcal{E}$ και $\mathcal{D}$, καθένα από τα οποία δέχεται στην είσοδό του $m + n$ δυαδικά ψηφία (m ψηφία του κλειδιού και n ψηφία ενός πακέτου) και παράγει στην έξοδο άλλα n ψηφία (ένα άλλο πακέτο), όπως στο Σχήμα 7. Το κάτι περισσότερο συνίσταται στο ότι η



Σχημα 7

κατασκευή θα πρέπει να τηρεί τις παρακάτω τέσσερις προδιαγραφές, κατά γνησίως φθίνουσα σειρά σπουδαιότητας:

Αντιστρεψιμότητα: Κάθε κρυπτογραφική πράξη που εκτελείται μέσα στο κουτί $\mathcal{E}$ πρέπει να είναι αντιστρέψιμη, ώστε το κουτί $\mathcal{D}$ να μπορεί τελικά, όταν τροφοδοτείται με το ίδιο κλειδί και το κρυπτοκείμενο, να ανακτά το αρχικό κείμενο εφαρμόζοντας τις αντίστροφες πράξεις. Διαφορετικά, τα δύο κουτιά δεν συνιστούν κρυπτοσύστημα.

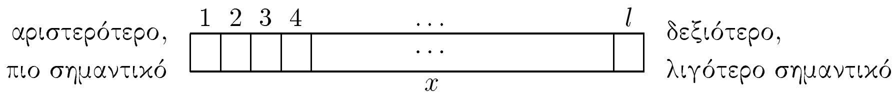
Ασφάλεια: Οι ακολουθίες των πράξεων που εφαρμόζονται μέσα στα κουτιά πρέπει να είναι τέτοιες ώστε να γίνεται όσο το δυνατόν δυσκολότερη η προσπάθεια του εχθρού να υπολογίσει το κλειδί που χρησιμοποιείται. Διαφορετικά, το κρυπτοσύστημα των δύο κουτιών δεν είναι ισχυρό.

Ταχύτητα: Οι ακολουθίες των πράξεων μέσα στα δύο κουτιά πρέπει να μπορούν να εκτελεστούν σε αρκετά μικρό χρόνο, ώστε να μπορούν να επιτευχθούν αρκετά υψηλοί ρυθμοί κρυπτογράφησης. Διαφορετικά, το κρυπτοσύστημα δεν είναι πρακτικό.

Απλότητα: Οι ακολουθίες των πράξεων μέσα στα δύο κουτιά πρέπει να είναι συνολικά όσο το δυνατόν απλούστερες. Διαφορετικά, το κρυπτοσύστημα δεν είναι φθηνό.

3.1. Στοιχειώδεις πράξεις. Οι στοιχειώδεις πράξεις που χρησιμοποιούνται για την κατασκευή των κουτιών δεν είναι πάρα πολλές, και αυτό που διαφοροποιεί τα κρυπτοσυστήματα πακέτου μεταξύ τους δεν είναι τόσο το ποιες πράξεις χρησιμοποιούν όσο το πώς συνδυάζουν αυτές τις πράξεις μεταξύ τους. Στην απαρίθμηση που ακολουθεί, βολεύει να θεωρήσουμε το κλειδί σαν μια σταθερά, παράμετρο του κάθε κουτιού, και όχι σαν μια μεταβλητή στην είσοδό του. Μιλάμε λοιπόν για τις πράξεις που χρησιμοποιούνται στην κατασκευή των συναρτήσεων e_k και d_k, για το τυχόν $k \in \mathcal{K} = \mathbb{B}^m$.

Εξάλλου, για κάθε $l \geq 1$ και για κάθε ακολουθία ψηφίων $x \in \mathbb{B}^l$, θεωρούμε τα ψηφία της x αριθμημένα έτσι ώστε το αριστερότερο (πιο σημαντικό) ψηφίο να έχει



αύξοντα αριθμό 1 και το δεξιότερο (λιγότερο σημαντικό) να έχει αύξοντα αριθμό l. Παρόμοια, η αρίθμηση των γραμμών και των στηλών όλων των πινάκων και των διανυσμάτων ξεκινάει από το 1. Τέλος, όπου δεν δημιουργείται σύγχυση, δεν θα κάνουμε τη διάκριση ανάμεσα σε έναν ακέραιο και την ακολουθία δυαδικών ψηφίων που τον αναπαριστά στο δυαδικό σύστημα· π.χ., επιτρέπεται να μιλάμε για τη διαφορά $x - 3$, όταν $x \in \mathbb{B}^l$.

3.1.1. *Δυαδικές πράξεις (bitwise operators).* Οι πιο συνηθισμένες τέτοιες πράξεις είναι η (αποκλειστική) διάζευξη και οι περιστροφές.

Η διάζευξη είναι η γνωστή συνάρτηση δύο μεταβλητών

$$\oplus : \mathbb{B}^{\,l} \times \mathbb{B}^{\,l} \to \mathbb{B}^{\,l},$$

για κάποιο $l \geq 1$, που σε κάθε δύο $x, y \in \mathbb{B}^{\,l}$ επιστρέφει ως $x \oplus y$ την ακολουθία που έχει ως i-οστό ψηφίο ($i = 1, \dots, l$) το άθροισμα (modulo 2) των i-οστών ψηφίων των x και y. Είναι εύκολο να επαληθεύσει κανείς ότι με αυτήν την πράξη το $\mathbb{B}^{\,l}$ γίνεται αβελιανή ομάδα με ουδέτερο στοιχείο την ακολουθία 0^l των l μηδενικών και με αντίστροφο κάθε ακολουθίας την ίδια την ακολουθία. Αυτό πρακτικά σημαίνει ότι μπορούμε, π.χ., την εξίσωση

$$\big((x_3 \oplus x_4) \oplus (x_1 \oplus x_2)\big) \oplus x_5 = y_1 \oplus (y_2 \oplus y_3)$$

να την γράφουμε κατευθείαν και ισοδύναμα ως

$$x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 = y_1 \oplus y_2 \oplus y_3$$

(δηλαδή να διώξουμε όλες τις παρενθέσεις και να αλλάξουμε τη σειρά των μεταβλητών) αλλά και ως

$$x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus y_1 \oplus y_2 \oplus y_3 = 0^l$$

(δηλαδή να φέρουμε όλες τις μεταβλητές στο ένα μέλος και να αφήσουμε στο άλλο μέλος το 0^l).

Συχνά, η πράξη εμφανίζεται με το ένα από τα ορίσματά της σταθερό, δηλαδή ως η συνάρτηση μιας μεταβλητής

$$\oplus_u : \mathbb{B}^{\,l} \to \mathbb{B}^{\,l}, \qquad \text{με} \quad \oplus_u(x) = x \oplus u,$$

για κάποιο $u \in \mathbb{B}^{\,l}$, και τότε βέβαια είναι μια αντιστοιχία με αντίστροφή της το εαυτό της. Επιπλέον, τις περισσότερες φορές η σταθερά u είναι συνάρτηση του κλειδιού k (συνηθέστερα, μια επιλογή ψηφίων του k). Τότε λέμε ότι η $\oplus_u$ είναι μια συνάρτηση *λεύκανσης* (whitening).[5]

Οι περιστροφές είναι οι γνωστές πράξεις

$$\lll : \mathbb{B}^{\,l} \times \{0, \dots, l-1\} \to \mathbb{B}^{\,l} \quad \text{και} \quad \ggg : \mathbb{B}^{\,l} \times \{0, \dots, l-1\} \to \mathbb{B}^{\,l},$$

για κάποιο $l \geq 1$, που για κάθε $x \in \mathbb{B}^{\,l}$ και κάθε $i = 0, \dots, l-1$ επιστρέφουν ως $x \lll i$ και $x \ggg i$ τις ακολουθίες που προκύπτουν από την κυκλική περιστροφή της x κατά i ψηφία προς τα αριστερά ή δεξιά, αντίστοιχα. Όταν το μήκος l των ακολουθιών δεν είναι σαφές, θα γράφουμε τις $\lll$, $\ggg$ και ως $\lll_l$, $\ggg_l$. Είναι προφανές ότι οι περιστροφές είναι αντιστοιχίες και μάλιστα $(\lll_l)^{-1} = \ggg_l$.

Στις περισσότερες περιπτώσεις, οι περιστροφές χρησιμοποιούνται με το δεύτερο από τα ορίσματά τους σταθερό και μόνο πρόσφατα[6] αυτό το όρισμα άρχισε να εξαρτάται από τις εισόδους των συναρτήσεων e_k και d_k. Πρόκειται για μια σημαντική καινοτομία, μια και, όπως θα δούμε σε επόμενες ενότητες, η χρήση της μπορεί να κάνει τους αλγόριθμους πολύ πιο απλούς, και μάλιστα χωρίς συνέπειες στην ασφάλεια και την ταχύτητα.[7] Τότε μιλάμε για *εξαρτημένες περιστροφές* (data dependent

[5] Η ονομασία προέρχεται από το ότι η διάζευξη με ψηφία από το κλειδί κάνει το όρισμα να φαίνεται περισσότερο τυχαίο, και άρα να μοιάζει περισσότερο με τον *λευκό* θόρυβο.

[6] Κατά τον Rivest, πρώτα στο αλγόριθμο του [**15**] και μετά στο RC5 [**28**], οπότε και στο RC6 [**29**]. Επίσης, στον MARS [**37**].

[7] Είναι σημαντικό ότι σε πολλούς νέους επεξεργαστές, η πράξη της περιστροφής έχει σταθερό κόστος ακόμη και όταν το δεύτερο όρισμά της είναι μεταβλητό (δηλαδή άγνωστο κατά τη μεταγλώττιση).

rotations) —σε αντιδιαστολή με τις *σταθερές περιστροφές* (fixed rotations)— και το δεύτερο όρισμα μπορεί να είναι οποιαδήποτε ακολουθία δυαδικών ψηφίων, αλλά μόνο τα $\lg l$ δεξιότερα (λιγότερο σημαντικά) ψηφία της (ως αναπαράσταση μιας τιμής στο $\{0, \ldots, l-1\}$) λαμβάνονται υπόψη.

Άλλες δυαδικές πράξεις (π.χ., η συμπλήρωση) δεν είναι δημοφιλείς. Βεβαίως, για τις περισσότερες από αυτές (απλή διάζευξη, σύζευξη, ολισθήσεις, κλπ.), ο λόγος που δεν χρησιμοποιούνται είναι το γεγονός ότι δεν είναι αντιστοιχίες, και έτσι εμποδίζουν την αντιστρεψιμότητα του αποτελέσματος.

3.1.2. *Αριθμητικές πράξεις.* Κυρίως χρησιμοποιείται η συνήθης πρόσθεση modulo 2^l

$$+ : \mathbb{B}^{\,l} \times \mathbb{B}^{\,l} \to \mathbb{B}^{\,l},$$

για κάποιο $l \geq 1$. Όταν το ένα από τα δύο ορίσματά της είναι σταθερό, η πράξη είναι βεβαίως μια αντιστοιχία ως προς το μεταβλητό όρισμα και η αντίστροφή της είναι η αφαίρεση (modulo 2^l, πάλι) κατά το σταθερό όρισμα.

3.1.3. *Επιλογές.* Αν $l_1, l_2 \geq 1$, τότε κάθε $1 \times l_2$ διάνυσμα A με στοιχεία από το $\{1, \ldots, l_1\}$ ορίζει τη συνάρτηση

$$\varepsilon_A : \mathbb{B}^{\,l_1} \to \mathbb{B}^{\,l_2}$$

που για κάθε $x \in \mathbb{B}^{\,l_1}$ επιστρέφει την ακολουθία

$$\varepsilon_A(x) = \text{η ακολουθία του } \mathbb{B}^{\,l_2} \text{ που για κάθε } i = 1, \ldots, l_2 \text{ έχει ως } \\ i\text{-οστό της ψηφίο το } A[i]\text{-οστό ψηφίο της } x.$$

Λέμε ότι η ε_A είναι μια *επιλογή*. Παραδείγματος χάριν, αν $l_1 = 8$, $l_2 = 5$ και $A = [3, 4, 8, 1, 6]$, τότε $\varepsilon_A(00110101) = 11101$.

Είναι φανερό ότι:

- Αν $l_1 > l_2$, κάποια από τα ψηφία της x δεν αντιγράφονται στην $\varepsilon_A(x)$. Τότε λέμε ότι η ε_A είναι μια *σύμπτυξη*.
- Αν $l_1 < l_2$, κάποια από τα ψηφία της x αντιγράφονται περισσότερες από μία φορές στην $\varepsilon_A(x)$. Τότε λέμε ότι η ε_A είναι μια *επέκταση*.
- Αν $l_1 = l_2$, τότε είναι δυνατόν κάθε ψηφίο της x να αντιγράφεται ακριβώς μία φορά στην $\varepsilon_A(x)$. Αν πράγματι συμβαίνει αυτό, τότε το διάνυσμα A είναι μια μετάθεση του $\{1, \ldots, l\}$ $(l = l_1 = l_2)$ και η ε_A είναι μια *μετάθεση* του $\mathbb{B}^{\,l}$.

Τέλος, δύο βασικές (όσο και προφανείς) ιδιότητες των επιλογών είναι ότι επιμερίζονται ως προς τη διάζευξη

$$\varepsilon_A(x \oplus y) = \varepsilon_A(x) \oplus \varepsilon_A(y)$$

και ότι συντιθέμενες μεταξύ τους παράγουν πάλι επιλογές.

3.1.4. *Συναρτήσεις απόσπασης.* Μια ειδική περίπτωση επιλογής είναι η πράξη που από μια ακολουθία 32 ψηφίων ξεχωρίζει και επιστρέφει την τρίτη (από αριστερά προς τα δεξιά) τετράδα. Είναι φανερό ότι πρόκειται για την επιλογή $\varepsilon_{[9,10,11,12]}$.

Στη γενική περίπτωση, έχουμε να κάνουμε με την πράξη που χωρίζει μια ακολουθία μήκους n σε $\frac{n}{m}$ διαδοχικές υπακολουθίες μήκους m, για κάποιο m που διαιρεί το n, και επιστρέφει τη j-οστή από αυτές (από τα αριστερά προς τα δεξιά), για κάποιο $j \in \{1, 2, \ldots, \frac{n}{m}\}$. Τότε πρόκειται για την επιλογή ε_A, με

$$A = [(j-1)m + 1, (j-1)m + 2, \ldots, jm].$$

Συμβολίζουμε αυτή την πράξη με το σύμβολο $\cdot_{j,m}$, και λέμε ότι είναι μια *απόσπαση*. Ώστε, για το συγκεκριμένο διάνυσμα A,

$$\cdot_{j,m} : \mathbb{B}^{\,n} \to \mathbb{B}^{\,m}, \qquad \text{με} \quad x_{j,m} = \varepsilon_A(x).$$

Ειδικές περιπτώσεις απόσπασης αποτελούν οι πράξεις που επιστρέφουν το αριστερό ή το δεξί μισό μιας ακολουθίας άρτιου μήκους. Τις συμβολίζουμε με $\cdot^L$ και $\cdot^R$ αντίστοιχα. Δηλαδή, για άρτιο n,

$$\cdot^L = \cdot_{1,n/2} : \mathbb{B}^n \to \mathbb{B}^{n/2} \qquad \text{και} \qquad \cdot^R = \cdot_{2,n/2} : \mathbb{B}^n \to \mathbb{B}^{n/2}.$$

3.1.5. *Ανταλλαγή μισών.* Μια ειδική περίπτωση μετάθεσης είναι η πράξη που, δεδομένης μια ακολουθίας x άρτιου μήκους, επιστρέφει την ακολουθία που προκύπτει όταν αλλάξουμε θέση στα δύο μισά (αριστερό και δεξί) της x. Συμβολίζουμε αυτην τη πράξη με το σύμβολο $\circlearrowleft$. Ώστε, για άρτιο n,

$$\circlearrowleft : \mathbb{B}^n \to \mathbb{B}^n \qquad \text{με} \quad \circlearrowleft x = \varepsilon_A(x),$$

όπου $A = [\frac{n}{2}+1, \ldots, n, 1, \ldots, \frac{n}{2}]$. Και προφανώς $\circlearrowleft^{-1} = \circlearrowleft$.

3.1.6. *Παράθεση.* Η παράθεση είναι η πράξη της συνένωσης δυο δυαδικών ακολουθιών σε μία καινούρια, δηλαδή η συνάρτηση

$$\| : \mathbb{B}^{l_1} \times \mathbb{B}^{l_2} \to \mathbb{B}^{l_1+l_2} \qquad \text{με} \quad x \,\|\, y = xy,$$

για οποιαδήποτε $l_1, l_2 \geq 1$.

3.1.7. *Αντικαταστάσεις.* Αν $l_1, l_2, l_3 \geq 1$, τότε κάθε $2^{l_1} \times 2^{l_2}$ πίνακας A με στοιχεία από το $\{0, \ldots, 2^{l_3} - 1\}$ ορίζει τη συνάρτηση

$$\alpha_A : \mathbb{B}^{l_1+l_2} \to \mathbb{B}^{l_3}$$

που, για κάθε $x \in \mathbb{B}^{l_1}$ και $y \in \mathbb{B}^{l_2}$, επιστρέφει για την ακολουθία xy την ακολουθία

$$\alpha_A(xy) = A[x+1, y+1].$$

Π.χ., αν $l_1 = 1$, $l_2 = 2$, $l_3 = 3$ και $A = \left(\begin{smallmatrix} 001 & 011 & 111 & 101 \\ 101 & 010 & 000 & 110 \end{smallmatrix}\right)$, τότε $\alpha_A(110) = 000$. Προφανώς, η α_A είναι αντιστρέψιμη μόνο αν $l_1 + l_2 = l_3$, όμως αυτή του παραδείγματος δεν είναι. Τον πίνακα A τον ονομάζουμε και *πίνακα αντικατάστασης* (substitution box, s-box).

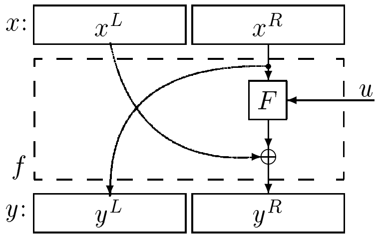
Οι πίνακες αντικατάστασης ενός κρυπτοσυστήματος μπορούν να είναι σταθεροί ή να εξαρτώνται από το κλειδί k (*εξαρτημένοι πίνακες αντικατάστασης* (key dependent s-boxes))[8] και συνιστούν ένα από τα πιο σημαντικά είδη πράξεων. Όταν είναι καλά σχεδιασμένοι, αποτελούν τη βασική άμυνα του κρυπτοσυστήματος απέναντι σε πολύ ισχυρές τακτικές κρυπτανάλυσης, όπως η διαφορική.[9] Όμως κάποια νέα συστήματα τους έχουν ήδη εγκαταλείψει, στηρίζοντας πλέον την ασφάλειά τους στις εξαρτημένες περιστροφές που, παρότι πολύ απλούστερες, (μοιάζουν να) είναι τουλάχιστον το ίδιο ανθεκτικές απέναντι στην κρυπτανάλυση.

3.2. Δίκτυα Feistel (Feistel networks). Τώρα που ξέρουμε τους στοιχειώδεις τελεστές που έχουμε στη διάθεσή μας, μπορούμε να δούμε πώς αυτοί συνδυάζονται για δώσουν πιο πολύπλοκους μετασχηματισμούς.

Μια από τις πιο παλιές τεχνικές για αυτή τη δουλειά είναι η τεχνική των Feistel δικτύων, που πήραν το όνομά τους από τον άνθρωπο που τα πρωτοπεριέγραψε (δημόσια, τουλάχιστον) [**10**]. Με κατάλληλη επιλογή των παραμέτρων τους μπορούν να εξασφαλίσουν πολύ μεγάλη ασφάλεια και ταχύτητα, ενώ παράλληλα καθιστούν το σύστημα εξαιρετικά απλό, υπό την έννοια ότι οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης είναι σχεδόν όμοιοι. Κάθε τέτοιο δίκτυο έχει τρεις βασικές ακέραιες παραμέτρους, $n, l, r \geq 1$, ο ρόλος των οποίων θα εξηγηθεί στη συνέχεια. Η n πρέπει να είναι άρτια.

[8] Για παράδειγμα, είναι σταθεροί στο DES, αλλά εξαρτημένοι στο Twofish.

[9] Π.χ., παράβαλε την Πρόταση 4-3.



Σχημα 8. Ένας γύρος Feistel πάνω από τη συνάρτηση F.

Το πρώτο πράγμα που πρέπει να έχει κανείς στη διάθεσή του για να κατασκευάσει ένα Feistel δίκτυο είναι μια συνάρτηση

$$F : \mathbb{B}^{n/2} \times \mathbb{B}^{l} \to \mathbb{B}^{n/2},$$

όπου n, l οι επιλεγμένοι παράμετροι για το δίκτυο. Πέρα από το να είναι γρήγορα υπολογίσιμη, η F δεν υποχρεούται να έχει καμιά άλλη ιδιότητα (π.χ., μονομορφικότητα, αντιστρεψιμότητα). Επειδή συχνά θα θεωρούμε για ευκολία το δεύτερο όρισμά της ως παράμετρο, εισάγουμε από τώρα το συμβολισμό F_u για τη συνάρτηση

$$x \mapsto F(x, u)$$

και για οποιοδήποτε $u \in \mathbb{B}^{l}$.

Με την F διαθέσιμη, μπορούμε να κατασκευάσουμε το βασικό συστατικό του δικτύου: ένα *γύρο Feistel* (Feistel round) (Σχήμα 8). Ο γύρος δέχεται σαν είσοδο ένα πακέτο x και μια εξαρτώμενη από το κλειδί ακολουθία l ψηφίων, το *υποκλειδί* (subkey) u. Η έξοδός του είναι ένα νέο πακέτο y, που υπολογίζεται ως εξής: Το αριστερό του μισό y^L είναι το δεξί μισό x^R του πακέτου εισόδου. Και το δεξιό του μισό y^R είναι η διάζευξη του αριστερού μισού x^L του πακέτου εισόδου με την τιμή που επιστρέφει η συνάρτηση F για το υποκλειδί u και το δεξί μισό x^R του x. Επομένως, ένας γύρος Feistel είναι η συνάρτηση

$$f : \mathbb{B}^{n} \times \mathbb{B}^{l} \to \mathbb{B}^{n}$$

που για κάθε $x \in \mathbb{B}^{n}$ και $u \in \mathbb{B}^{l}$ επιστρέφει την τιμή

$$f(x, u) = x^R \,\|\, x^L \oplus F(x^R, u).$$

Και πάλι, θα συμφέρει να εμφανίζουμε το δεύτερο όρισμα της f ως παράμετρο, οπότε ονομάζουμε από τώρα f_u τη συνάρτηση $x \mapsto f(x, u)$, ώστε για κάθε $u \in \mathbb{B}^{l}$ είναι

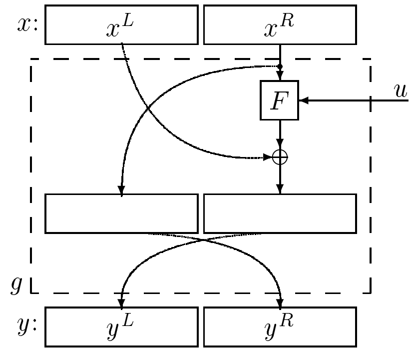
$$f_u : \mathbb{B}^{n} \to \mathbb{B}^{n}, \quad \text{με} \quad f_u(x) = x^R \,\|\, x^L \oplus F_u(x^R).$$

Και είναι εύκολη η επόμενη παρατήρηση.

3.1. Προταση. *Για κάθε $u \in \mathbb{B}^{l}$, η f_u είναι μια μετάθεση του $\mathbb{B}^{n}$. Η αντίστροφη μετάθεση δίνεται από τον τύπο*

$$f_u^{-1}(y) = y^R \oplus F_u(y^L) \,\|\, y^L. \tag{2}$$

Αποδειξη. Έστω ότι $x_1 \neq x_2$ και $y_1 = f_u(x_1)$, $y_2 = f_u(x_2)$. Αν $x_1^R \neq x_2^R$, τότε $y_1^L \neq y_2^L$ και επομένως $y_1 \neq y_2$. Αν αντίθετα $x_1^R = x_2^R$, τότε $F_u(x_1^R) = F_u(x_2^R)$ και $x_1^L \neq x_2^L$, άρα $x_1^L \oplus F_u(x_1^R) \neq x_2^L \oplus F_u(x_2^R)$, δηλαδή $y_1^R \neq y_2^R$, και επομένως ξανά $y_1 \neq y_2$. Άρα η f_u είναι μονομορφισμός.



Σχημα 9. Δίκτυο Feistel ενός γύρου.

Εξάλλου, για το τυχόν $y \in \mathbb{B}^n$, υπάρχει το πακέτο $x = y^R \oplus F_u(y^L) \,\|\, y^L$ και είναι εύκολο να επιβεβαιώσουμε ότι $f_u(x) = y$. Οπότε η f_u είναι και επιμορφική.

Άρα η f_u είναι μια αντιστοιχία του $\mathbb{B}^n$ στο $\mathbb{B}^n$, δηλαδή μια μετάθεσή του. Και, από τον τρόπο που υπολογίσαμε το x της προηγούμενης παραγράφου, έπεται ότι η αντίστροφη μετάθεση έχει τον τύπο (2). ⊣

Αλλά ο τύπος της f_u^{-1} μοιάζει αρκετά με τον τύπο της f_u. Αυτό δεν είναι τυχαίο και μπορεί να γίνει πιο συγκεκριμένο.

3.2. Προταση. *Για κάθε* $u \in \mathbb{B}^l$, *ισχύει ότι*

$$f_u^{-1} \circ \circlearrowleft = \circlearrowleft \circ f_u.$$

Αποδειξη. Για κάθε $y \in \mathbb{B}^n$, υπολογίζουμε

$$\begin{aligned} f_u^{-1}(\circlearrowleft y) &= (\circlearrowleft y)^R \oplus F_u\big((\circlearrowleft y)^L\big) \,\|(\circlearrowleft y)^L \\ &= y^L \oplus F_u(y^R) \,\|\, y^R \\ &= \circlearrowleft\big(y^R \,\|\, y^L \oplus F_u(y^R)\big) \\ &= \circlearrowleft\big(f_u(y)\big), \end{aligned}$$

το οποίο επιβεβαιώνει τον ισχυρισμό. ⊣

Αυτό σημαίνει ότι, για κάθε $u \in \mathbb{B}^l$, η συνάρτηση $g_u = \circlearrowleft \circ f_u$, που περιγράφεται στο Σχήμα 9, είναι αντίστροφη του εαυτού της. Γιατί

$$g_u^{-1} = (\circlearrowleft \circ f_u)^{-1} = f_u^{-1} \circ \circlearrowleft^{-1} = f_u^{-1} \circ \circlearrowleft = \circlearrowleft \circ f_u = g_u.$$

Αν λοιπόν σε ένα κρυπτοσύστημα πακέτου με διαστάσεις $n \times l$ η συνάρτηση κρυπτογράφησης είναι η $e_k = g_k$, τότε η συνάρτηση αποκρυπτογράφησης είναι η $d_k = e_k^{-1} = e_k$ και πάλι. Δηλαδή το ίδιο πρόγραμμα (ή το ίδιο ολοκληρωμένο κύκλωμα) θα κάνει και την κρυπτογράφηση και την αποκρυπτογράφηση. Αυτό σίγουρα είναι ένα αποφασιστικό βήμα προς την απλότητα του κρυπτοσυστήματος συνολικά. Και είναι σημαντικό το ότι ισχύει, όποια κι είναι η συνάρτηση F που έχουμε διαλέξει αρχικά.

Όμως είναι εύκολο να διαπιστώσουμε ότι μια συνάρτηση σαν αυτή του Σχήματος 9 δεν μπορεί να προσφέρει την ασφάλεια που ζητάμε, αν η συνάρτηση F δεν γίνει εξαιρετικά πολύπλοκη. Ευτυχώς, υπάρχει τρόπος να διατηρήσουμε την απλότητα χωρίς να χάσουμε σε ασφάλεια. Και αυτός βασίζεται σε μια γενίκευση της μέχρι τώρα ιδέας.

3.3. Πρόταση. *Για κάθε $r \geq 1$ και κάθε $u_1, \ldots, u_r \in \mathbb{B}^l$, ισχύει ότι*

$$f_{u_r}^{-1} \circ \cdots \circ f_{u_1}^{-1} \circ \circlearrowleft = \circlearrowleft \circ f_{u_r} \circ \cdots \circ f_{u_1}.$$

Απόδειξη. Επαγωγικά στο r. Αν $r = 1$, το αποτέλεσμα είναι η Πρόταση 3.2. Αν $r > 1$, τότε

$$\begin{aligned} f_{u_r}^{-1} \circ \cdots \circ f_{u_2}^{-1} \circ f_{u_1}^{-1} \circ \circlearrowleft &= f_{u_r}^{-1} \circ \cdots \circ f_{u_2}^{-1} \circ \circlearrowleft \circ f_{u_1} \quad &\text{(από την Πρόταση 3.2)} \\ &= \circlearrowleft \circ f_{u_r} \circ \cdots \circ f_{u_2} \circ f_{u_1}, \quad &\text{(επαγωγική υπόθεση)} \end{aligned}$$

κι έτσι το ζητούμενο ισχύει. ⊣

Επομένως, για κάθε $u_1, \ldots, u_r \in \mathbb{B}^l$, η συνάρτηση του Σχήματος 10

$$g_{u_1,\ldots,u_r} = \circlearrowleft \circ f_{u_r} \circ \cdots \circ f_{u_1},$$

έχει την ιδιότητα ότι

$$\begin{aligned} g_{u_1,\ldots,u_r}^{-1} &= (\circlearrowleft \circ f_{u_r} \circ \cdots \circ f_{u_1})^{-1} \\ &= f_{u_1}^{-1} \circ \cdots \circ f_{u_r}^{-1} \circ \circlearrowleft^{-1} \\ &= f_{u_1}^{-1} \circ \cdots \circ f_{u_r}^{-1} \circ \circlearrowleft \\ &= \circlearrowleft \circ f_{u_r} \circ \cdots \circ f_{u_1} \\ &= g_{u_r,\ldots,u_1}. \end{aligned}$$

Δηλαδή, για να αντιστρέψουμε την $g_{u_1,\ldots,u_r}$ αρκεί να αντιστρέψουμε τη σειρά των παραμέτρων της. Δηλαδή τη σειρά με την οποία δίνουμε τις τιμές $u_1, \ldots, u_r$ στα r αντίγραφα της F μέσα στο υπολογιστικό διάγραμμα της συνάρτησης στο Σχήμα 10.

Αν λοιπόν σε ένα κρυπτοσύστημα πακέτου με διαστάσεις $n \times m$ η συνάρτηση κρυπτογράφησης είναι η $e_k = g_{u_1,\ldots,u_r}$, όπου τα $u_1, \ldots, u_r \in \mathbb{B}^l$ είναι συναρτήσεις του κλειδιού k, τότε η συνάρτηση αποκρυπτογράφησης είναι απλώς η $d_k = e_k^{-1} = g_{u_r,\ldots,u_1}$, και μπορεί να υπολογιστεί από το ίδιο πρόγραμμα (ή ολοκληρωμένο κύκλωμα) που υπολογίζει την e_k, με μόνη τροποποίηση την αντιστροφή της σειράς με την οποία τροφοδοτούνται οι παράμετροι στα F-κουτιά (Σχήμα 11).

Τώρα μπορούμε να κάνουμε πιο συγκεκριμένο το τι ακριβώς έχουμε ορίσει και το τι έχουμε αποδείξει για αυτό.

3.4. Ορισμός. Θεωρούμε τυχόντες ακέραιους $n, l \geq 1$, με το n άρτιο, και τυχούσα συνάρτηση

$$F : \mathbb{B}^{n/2} \times \mathbb{B}^l \to \mathbb{B}^{n/2}.$$

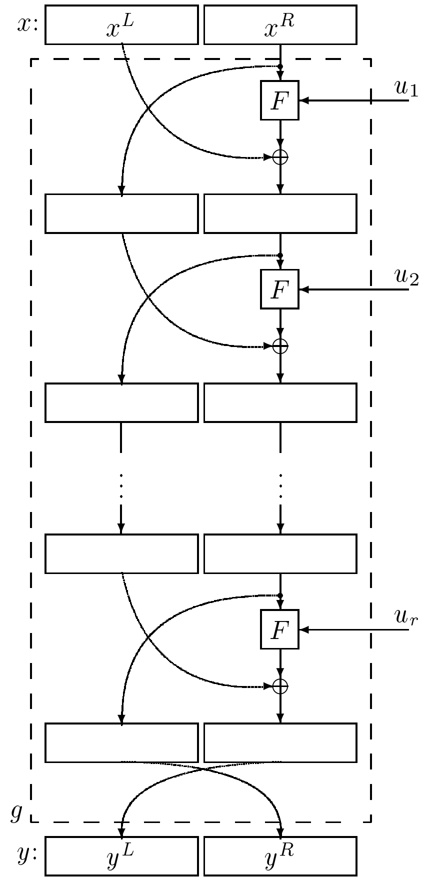
Η συνάρτηση

$$f : \mathbb{B}^n \times \mathbb{B}^l \to \mathbb{B}^n, \qquad \text{με} \quad f(x, u) = x^R \parallel x^L \oplus F(x^R, u)$$

λέγεται *Feistel γύρος πάνω από την* F (Σχήμα 8). Επιπλέον, για κάθε $u \in \mathbb{B}^l$, λέμε ότι η συνάρτηση

$$f_u : \mathbb{B}^n \to \mathbb{B}^n, \qquad \text{με} \quad f_u(x) = f(x, u)$$

είναι η *Feistel μετάθεση πάνω από την F που ορίζει το u.*



Σχημα 10. Δίκτυο Feistel r γύρων.

3.5. Ορισμος. Θεωρούμε τυχόντες ακέραιους $n, l, r \geq 1$, με το n άρτιο, και τυχούσα συνάρτηση

$$F : \mathbb{B}^{n/2} \times \mathbb{B}^{l} \to \mathbb{B}^{n/2}.$$

Λέμε *Feistel δίκτυο r γύρων πάνω από την F* τη συνάρτηση

$$\mathcal{F} : \mathbb{B}^{n} \times (\mathbb{B}^{l})^{r} \to \mathbb{B}^{n}$$

που για κάθε $x \in \mathbb{B}^{n}$ και $u_1, \ldots, u_r \in \mathbb{B}^{l}$ επιστρέφει την τιμή

$$\mathcal{F}(x, u_1, \ldots, u_r) = (\circlearrowleft \circ f_{u_r} \circ \cdots \circ f_{u_1})(x),$$

όπου f_{u_i} είναι η Feistel μετάθεση πάνω από την F που ορίζει το u_i, για κάθε $i = 1, \ldots, r$ (Σχήμα 10). Λέμε ότι το $\mathcal{F}$ έχει διαστάσεις $n \times l \times r$.

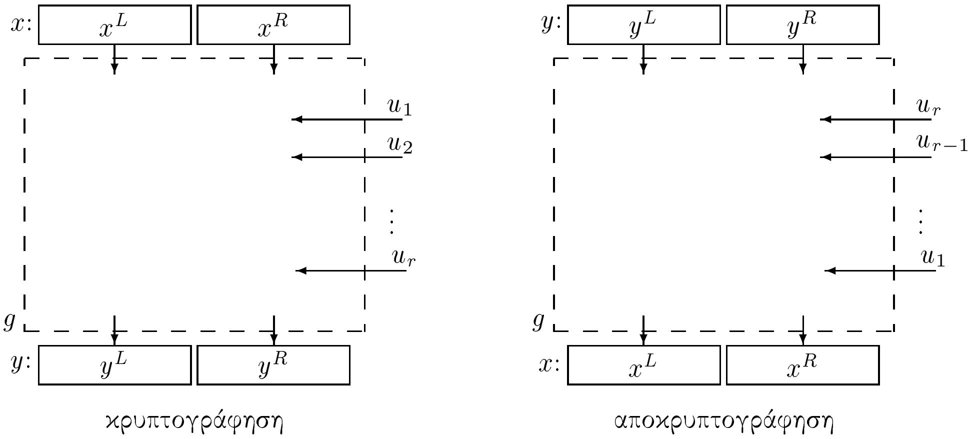
Επιπλέον, για κάθε $u_1, \ldots, u_r$ στο $\mathbb{B}^{l}$, λέμε ότι η συνάρτηση

$$\mathcal{F}_{u_1,\ldots,u_r} : \mathbb{B}^{n} \to \mathbb{B}^{n}, \quad \text{με} \quad \mathcal{F}_{u_1,\ldots,u_r}(x) = \mathcal{F}(x, u_1, \ldots, u_r)$$

είναι η *Feistel πολυμετάθεση πάνω από την F που ορίζουν τα $u_1, \ldots, u_r$.*

3.6. Λημμα. *Κάθε Feistel μετάθεση f_u του Ορισμού 3.4 είναι μια μετάθεση του $\mathbb{B}^{n}$, που ικανοποιεί την*

$$f_u^{-1} \circ \circlearrowleft = \circlearrowleft \circ f_u.$$



Σχημα 11. Κρυπτογράφηση και αποκρυπτογράφηση με ένα δίκτυο Feistel r γύρων.

Και κάθε Feistel πολυμετάθεση $\mathcal{F}_{u_1,\ldots,u_r}$ *του Ορισμού* 3.5 *είναι μια μετάθεση του* $\mathbb{B}^n$*, που αντιστρέφεται από την Feistel πολυμετάθεση με την αντίστροφη σειρά ορισμάτων,*

$$(\mathcal{F}_{u_1,\ldots,u_r})^{-1} = \mathcal{F}_{u_r,\ldots,u_1}.$$

Απόδειξη. Η συζήτηση που προηγήθηκε. ⊣

ΚΕΦΑΛΑΙΟ 2

Data Encryption Standard

Όπως είδαμε στην Ενότητα 1-1, ένα κρυπτοσύστημα πακέτου μπορεί να έχει οποιεσδήποτε διαστάσεις. Επίσης, οι στοιχειώδεις πράξεις που μπορούν να χρησιμοποιηθούν στην κατασκευή του είναι πάρα πολλές και οι στοιχειώδεις τρόποι για να τις οργανώσουμε είναι επίσης πολλοί. Είναι λοιπόν επόμενο καθένας που ξεκινά να κατασκευάσει ένα τέτοιο κρυπτοσύστημα να καταλήγει και σε ένα διαφορετικό, με πιθανότατα άλλες διαστάσεις από αυτά των άλλων κατασκευαστών, και σχεδόν πάντα με άλλα χαρακτηριστικά όσον αφορά την ασφάλεια, την ταχύτητα και την απλότητα.

Όμως, για να μπορέσουν να επικοινωνήσουν, δύο μέρη πρέπει να χρησιμοποιήσουν *το ίδιο* κρυπτοσύστημα. Και αυτό γίνεται πολύ δύσκολο όταν δεν υπάρχει ένα, μοναδικό και καθιερωμένο. Το ρόλο αυτό κλήθηκε να παίξει το πρότυπο που αναπτύχθηκε από την IBM και την NSA στη δεκαετία του '70 και τέθηκε σε ισχύ το 1977 από το αμερικανικό Υπουργείο Εμπορίου [**19**], με σκοπό την κρυπτογραφική προστασία *ευαίσθητων αλλά όχι απόρρητων* δεδομένων.

1. Περιγραφή

Το DES είναι ένα κρυπτοσύστημα πακέτου με διαστάσεις 64×56. Βασικό δομικό στοιχείο των συναρτήσεων κρυπτογράφησης και αποκρυπτογράφησης είναι ένα Feistel δίκτυο $\mathcal{F}$, διαστάσεων $64 \times 48 \times 16$.

1.1. Η συνάρτηση F. Η συνάρτηση πάνω από την οποία ορίζεται το $\mathcal{F}$ είναι η

$$F : \mathbb{B}^{32} \times \mathbb{B}^{48} \to \mathbb{B}^{32}, \qquad \text{με} \quad F(x,u) = \varepsilon_P\Big(S\big(\varepsilon_E(x) \oplus u\big)\Big),$$

που φαίνεται και στο Σχήμα 1. Περιγράφουμε τις συναρτήσεις ε_P, ε_E και S αμέσως μετά· πρώτα σημειώνουμε την παραμετρική εκδοχή της F:

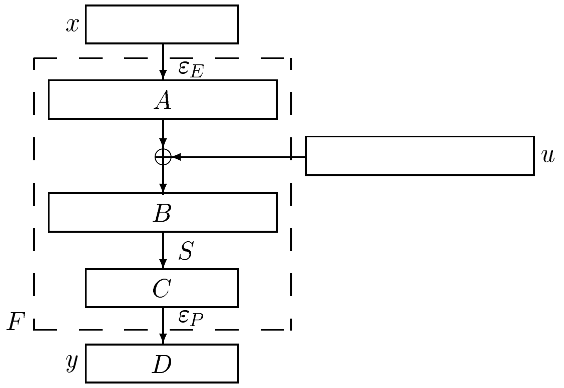
$$F_u : \mathbb{B}^{32} \to \mathbb{B}^{32}, \qquad \text{με} \quad F_u(x) = \varepsilon_P\Big(S\big(\oplus_u\big(\varepsilon_E(x)\big)\big)\Big), \tag{1}$$

για κάθε $u \in \mathbb{B}^{48}$.

Η συνάρτηση ε_P είναι η μετάθεση (των 32 ψηφίων) που ορίζεται από το διάνυσμα P του Πίνακα 1.

Η συνάρτηση ε_E είναι η επέκταση (των 32 ψηφίων σε 48) που ορίζεται από το διάνυσμα E του Πίνακα 2. Πρακτικά, το $\varepsilon_E(x)$ υπολογίζεται ως εξής (Σχήμα 2): Η 32-ψήφια ακολουθία x χωρίζεται σε 8 τετράδες. Καθεμιά από αυτές επεκτείνεται σε εξάδα, αντιγράφοντας απλώς το δεξιότερο ψηφίο της προηγούμενής της και το αριστερότερο ψηφίο της επόμενής της (ιδιαιτέρως, ως προηγούμενη της πρώτης τετράδας λογίζεται η τελευταία). Οι 8 εξάδες που προκύπτουν συνενώνονται με την ίδια σειρά για να δώσουν την επιστρεφόμενη 48-ψήφια ακολουθία.

Τέλος, η συνάρτηση $S : \mathbb{B}^{48} \to \mathbb{B}^{32}$ ορίζεται με βάση τους οχτώ πίνακες αντικατάστασης (s-boxes) $S_1, \dots, S_8$ του Πίνακα 5 (σελίδα 30): Αν $x \in \mathbb{B}^{48}$, για να υπολογίσουμε την $S(x)$ πρώτα χωρίζουμε τη x σε 8 εξάδες ψηφίων. Για κάθε



Σχημα 1. Η συνάρτηση F πάνω από την οποία ορίζεται το Feistel δίκτυο $\mathcal{F}$ του DES.

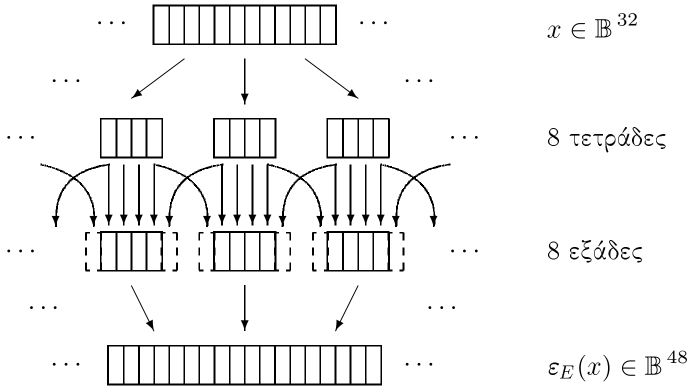
P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Πινακας 1. Το διάνυσμα P. Το πάνω αριστερά στοιχείο είναι το 1ο στοιχείο του διανύσματος και το κάτω δεξιά το 32ο.

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Πινακας 2. Το διάνυσμα E. Το πάνω αριστερά στοιχείο είναι το 1ο στοιχείο του διανύσματος και το κάτω δεξιά το 48ο.

$j = 1, \ldots, 8$, η j-οστή εξάδα (από αριστερά), έστω $b_1b_2b_3b_4b_5b_6$, ορίζει το στοιχείο $S_j[b_1b_6 + 1, b_2b_3b_4b_5 + 1]$ του πίνακα S_j (ώστε τα δύο εξωτερικά ψηφία της εξάδας προσδιορίζουν μια γραμμή και τα τέσσερα εσωτερικά μια στήλη του S_j). Έτσι παράγονται 8 τετράδες ψηφίων, που συνενωμένες με την ίδια σειρά δίνουν την 32-ψήφια



Σχημα 2. Υπολογισμός του $\varepsilon_E(x)$.

ακολουθία $S(x)$. Με την ορολογία της Ενότητας 1-3.1, η συνάρτηση S έχει τύπο

$$S(x) = \mathop{\Big\|}_{j=1}^{8} \alpha_{S_j}\Big(\varepsilon_Z(x_{j,6})\Big), \tag{2}$$

όπου α_{S_j} είναι η συνάρτηση αντικατάστασης που ορίζει ο πίνακας S_j και ε_Z η μετάθεση που ορίζει το διάνυσμα $Z = [1, 6, 2, 3, 4, 5]$ (ώστε τα ψηφία κάθε εξάδας $x_{j,6}$ να μπαίνουν στη σωστή σειρά πριν ερμηνευθούν από την α_{S_j}). Για ευκολία, θα συμβολίζουμε τη σύνθεση $\alpha_{S_j} \circ \varepsilon_Z$ με $\alpha_{S'_j}$, ώστε

$$S(x) = \mathop{\Big\|}_{j=1}^{8} \alpha_{S'_j}(x_{j,6}).$$

Όταν δεν υπάρχει σύγχυση για το ποιες ακριβώς είναι οι είσοδοι x και u, θα συμβολίζουμε τα αποτελέσματα των ενδιάμεσων υπολογισμών όπως στο Σχήμα 1, δηλαδή

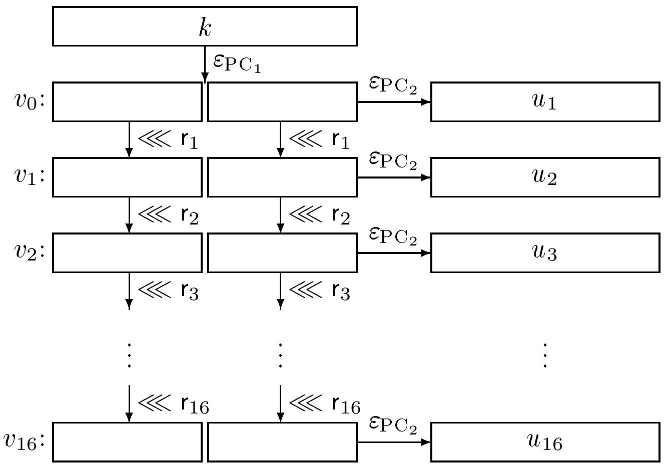
$$A = \varepsilon_E(x), \qquad B = \oplus_u(A), \qquad C = S(B), \qquad D = P(C). \tag{3}$$

1.2. Υποκλειδιά. Λέμε ότι καθεμιά από τις 16 48-ψήφιες παράμετρους του Feistel δικτύου που περιγράψαμε αποτελεί το *υποκλειδί* (subkey) του αντίστοιχου γύρου του δικτύου. Και όλα τα υποκλειδιά παράγονται από το κλειδί $k \in \mathbb{B}^{56}$ σύμφωνα με τη διαδικασία που φαίνεται στο Σχήμα 3 και εξηγούμε αμέσως τώρα.[1]

Αρχικά, τα ψηφία του κλειδιού μετατίθενται κατά τη μετάθεση $\varepsilon_{\mathrm{PC}_1}$, όπου PC_1 το διάνυσμα του Πίνακα 3. Το αποτέλεσμα χωρίζεται σε δύο κομμάτια, που υφίστανται ανεξάρτητα 16 διαδοχικές περιστροφές, κατά μία ή δύο θέσεις. Μετά από την i-οστή περιστροφή ($i = 1, \ldots, 16$), η σύμπτυξη $\varepsilon_{\mathrm{PC}_2}$ (όπου PC_2 το διάνυσμα του

[1]Το ακριβές είναι ότι το πρότυπο θεωρεί πως κάθε κλειδί έχει 64 ψηφία, με τα ψηφία 8, 16, 24, 32, 40, 48, 56 και 64 να είναι *ψηφία ισοτιμίας*, δηλαδή να έχουν απαραίτητα τέτοιες τιμές ώστε καθεμιά από τις ομάδες ψηφιών 1–8, 9–16, 17–24, 25–32, 33–40, 41–48, 49–56 και 57–64 να έχει άρτιο πλήθος μονάδων. Αυτό βεβαίως σημαίνει ότι τα συγκεκριμένα 8 ψηφία έχουν τιμές που καθορίζονται πλήρως από τα υπόλοιπα, κι έτσι δεν προσφέρουν στην ασφάλεια του κρυπτοσυστήματος.

Εδώ έχουμε αγνοήσει αυτή την τεχνική λεπτομέρεια και θεωρούμε από την αρχή ότι το κλειδί έχει μόνο τα υπόλοιπα $64 - 8 = 56$ ψηφία. Συνέπεια αυτού είναι και το γεγονός ότι τα διανύσματα PC_1 και PC_2 που φαίνονται στον Πίνακα 3 δεν είναι τα διανύσματα PC-1 και PC-2 που περιέχονται στο πρότυπο, αλλά κατάλληλες τροποποιήσεις τους. Γι' αυτό και η μικρή αλλαγή στο συμβολισμό.



Σχημα 3. Η διαδικασία παραγωγής των 16 υποκλειδιών από το κλειδί.

PC_1						
50	43	36	29	22	15	8
1	51	44	37	30	23	16
9	2	52	45	38	31	24
17	10	3	53	46	39	32
56	49	42	35	28	21	14
7	55	48	41	34	27	20
13	6	54	47	40	33	26
19	12	5	25	18	11	4

PC_2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Πινακας 3. Τα διανύσματα PC_1 και PC_2.

Πίνακα 3) διαλέγει 48 από τα 56 ψηφία των δύο κομματιών, παράγοντας έτσι το i-οστό υποκλειδί, u_i.

Πιο αναλυτικά, η διαδικασία υπολογίζει την ακολουθία $v = (v_i)_{0 \le i \le 16}$ που ορίζουν οι σχέσεις

$$v_0 = \varepsilon_{\mathrm{PC}_1}(k),$$
$$v_i = v_{i-1}^L \lll \mathsf{r}_i \,\|\, v_{i-1}^R \lll \mathsf{r}_i,$$

όταν οι σταθερές $\mathsf{r}_1, \ldots, \mathsf{r}_{16}$ που αποφασίζουν το ποσό της κάθε περιστροφής δίνονται από τον πίνακα

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
r_i	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Στη συνέχεια, για κάθε $i = 1, \ldots, 16$, το i-οστό υποκλειδί είναι το

$$u_i = \varepsilon_{\mathrm{PC}_2}(v_i).$$

Η παραπάνω διαδικασία είναι χρήσιμη όταν θέλουμε πραγματικά να *υπολογίσουμε* τα υποκλειδιά, γι' αυτό και περιγράφεται από το πρότυπο. Αν όμως μας ενδιαφέρει

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Πινακασ 4. Τα διανύσματα IP και IP^{-1}.

(όπως εδώ) μόνο να τα *ορίσουμε*, τότε υπάρχει απλούστερος τρόπος: Παρακολουθώντας την πορεία κάθε ψηφίου του κλειδιού δια μέσου των διαδοχικών περιστροφών και επιλογών, μπορούμε να βρούμε ποιο ψηφίο του κλειδιού αντιγράφεται στο κάθε ψηφίο του κάθε υποκλειδιού. Έτσι, υπολογίζουμε τα διανύσματα $R_1, \ldots, R_{16}$ των Πινάκων 6 και 7 (σελίδες 31 και 32), για τα οποία ισχύει ότι

$$u_i = \varepsilon_{R_i}(k),$$

για κάθε $i = 1, \ldots, 16$. Στο εξής θα θυμόμαστε μόνο αυτό για την παραγωγή των υποκλειδιών.

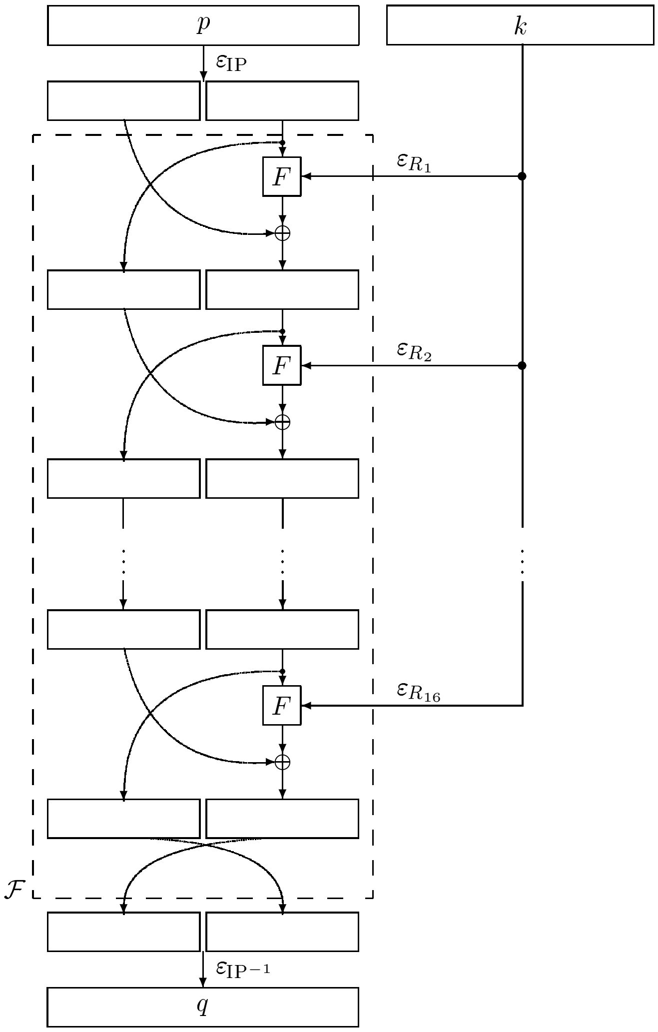
1.3. Οι συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης. Έχοντας ήδη περιγράφει το Feistel δίκτυο $\mathcal{F}$ και τον τρόπο κατασκευής των υποκλειδιών $u_1, \ldots, u_{16}$, μπορούμε τώρα να δούμε τον ορισμό της συνάρτησης κρυπτογράφησης. Σ' αυτόν συμμετέχουν η μετάθεση $\varepsilon_{\mathrm{IP}}$ και η αντίστροφή της, $\varepsilon_{\mathrm{IP}}^{-1} = \varepsilon_{\mathrm{IP}^{-1}}$, όπου IP (initial permutation) και IP^{-1} τα διανύσματα του Πίνακα 4.

Για το τυχόν κλειδί $k \in \mathbb{B}^{56}$ λοιπόν, η κρυπτογράφηση γίνεται μέσω της συνάρτησης (Σχήμα 4)

$$e_k = \varepsilon_{\mathrm{IP}^{-1}} \circ \mathcal{F}_{\varepsilon_{R_1}(k), \ldots, \varepsilon_{R_{16}}(k)} \circ \varepsilon_{\mathrm{IP}}.$$

Δηλαδή, το τυχόν $p \in \mathbb{B}^{64}$ περνάει διαδοχικά από τις μεταθέσεις $\varepsilon_{\mathrm{IP}}$, $\mathcal{F}_{\varepsilon_{R_1}(k), \ldots, \varepsilon_{R_{16}}(k)}$ και $\varepsilon_{\mathrm{IP}^{-1}}$. Για το ίδιο υποκλειδί, η συνάρτηση αποκρυπτογράφησης πρέπει βεβαίως να είναι η

$$\begin{aligned} d_k &= e_k^{-1} \\ &= (\varepsilon_{\mathrm{IP}^{-1}} \circ \mathcal{F}_{\varepsilon_{R_1}(k), \ldots, \varepsilon_{R_{16}}(k)} \circ \varepsilon_{\mathrm{IP}})^{-1} \end{aligned}$$



Σχημα 4. Η συνάρτηση κρυπτογράφησης του DES.

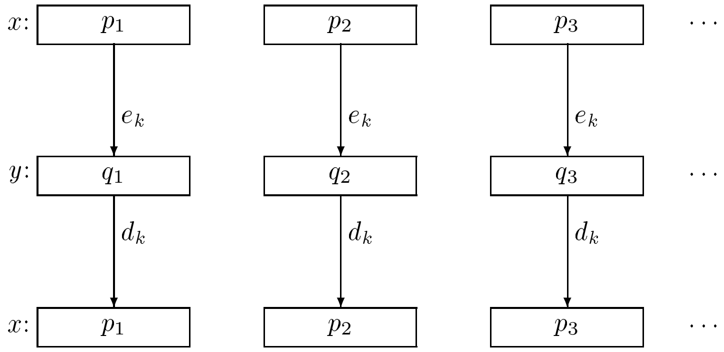
$$= \varepsilon_{\mathrm{IP}}^{-1} \circ \big(\mathcal{F}_{\varepsilon_{R_1}(k),\ldots,\varepsilon_{R_{16}}(k)}\big)^{-1} \circ \varepsilon_{\mathrm{IP}^{-1}}^{-1}$$
$$= \varepsilon_{\mathrm{IP}^{-1}} \circ \mathcal{F}_{\varepsilon_{R_{16}}(k),\ldots,\varepsilon_{R_1}(k)} \circ \varepsilon_{\mathrm{IP}}. \qquad \text{(Λήμμα 1-3.6)}$$

Οπότε, σύμφωνα προς τη φιλοσοφία των δικτύων Feistel, η αποκρυπτογράφηση γίνεται όπως και η κρυπτογράφηση (Σχήμα 4), με μόνη διαφορά την αντιστροφή της σειράς των υποκλειδιών.

Τελικά, είμαστε σε θέση να ορίσουμε το DES.

1.1. Ορισμος. Το Data Encryption Standard είναι το κρυπτοσύστημα πακέτου $(\mathbb{B}^{64}, \mathbb{B}^{64}, \mathbb{B}^{56}, \mathcal{E}, \mathcal{D})$, όπου

$$\mathcal{E} = \{e_k \mid k \in \mathbb{B}^{56}\}, \qquad \text{με} \quad e_k = \varepsilon_{\mathrm{IP}^{-1}} \circ \mathcal{F}_{\varepsilon_{R_1}(k),\ldots,\varepsilon_{R_{16}}(k)} \circ \varepsilon_{\mathrm{IP}},$$
$$\mathcal{D} = \{d_k \mid k \in \mathbb{B}^{56}\}, \qquad \text{με} \quad d_k = \varepsilon_{\mathrm{IP}^{-1}} \circ \mathcal{F}_{\varepsilon_{R_{16}}(k),\ldots,\varepsilon_{R_1}(k)} \circ \varepsilon_{\mathrm{IP}},$$



Σχημα 5. Χρήση του DES ως ηλεκτρονικού βιβλίου κωδικών. Το ένα από τα δύο κομμάτια δείχνει την κρυπτογράφηση (πάνω) και το άλλο την αποκρυπτογράφηση (κάτω).

τα διανύσματα $\mathrm{IP}, \mathrm{IP}^{-1}, R_1, \ldots, R_{16}$ δίνονται στους Πίνακες 4, 6, 7 και $\mathcal{F}$ είναι το 16 γύρων Feistel δίκτυο πάνω από την συνάρτηση F της Ενότητας 1.1.

2. Τρόποι λειτουργίας

2.1. Απλή λειτουργία. Όπως εξηγήσαμε στην Ενότητα 1-2, για να κρυπτογραφήσουμε μια δυαδική ακολουθία x μήκους N με ένα κρυπτοσύστημα πακέτου διαστάσεων $n \times m$, πρέπει πρώτα να την σπάσουμε σε $\nu = \frac{N}{n}$ πακέτα των n ψηφίων το καθένα,[2]

$$x = p_1 p_2 \cdots p_\nu,$$

και ακολούθως να κρυπτογραφήσουμε κάθε πακέτο χωριστά. Έτσι, το κρυπτογραφημένο μήνυμα είναι η ακολουθία κρυπτοπακέτων

$$y = q_1 q_2 \cdots q_\nu,$$

με

$$q_i = e_k(p_i), \qquad \text{για κάθε } i = 1, \ldots, \nu, \tag{ECB$_\mathrm{e}$}$$

και η αποκρυπτογράφησή του γίνεται με την προφανή χρήση της d_k,

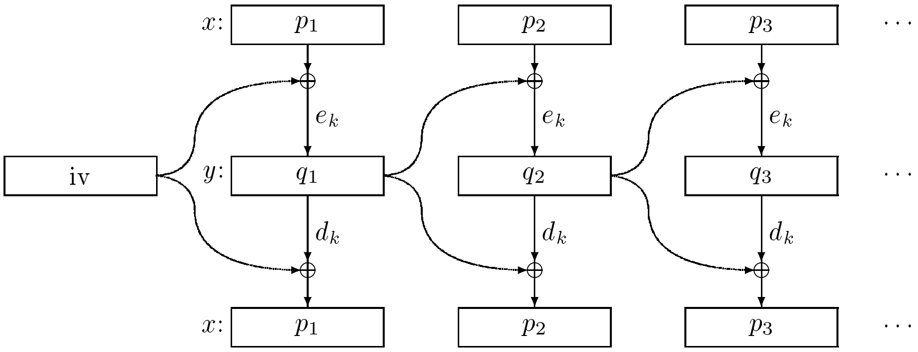
$$p_i = d_k(q_i), \qquad \text{για κάθε } i = 1, \ldots, \nu. \tag{ECB$_\mathrm{d}$}$$

Τα ίδια ισχύουν και για το DES.

Αυτός όμως είναι μόνο ένας (ο απλούστερος και ταχύτερος) από τους τρόπους με τους οποίους μπορούμε να χρησιμοποιήσουμε ένα κρυπτοσύστημα πακέτου. Και ονομάζεται *λειτουργία ηλεκτρονικού βιβλίου κωδικών* (electronic codebook mode, ECB mode), ακριβώς γιατί χρησιμοποιεί το κρυπτοσύστημα ως ένα βιβλίο-«πίνακα αντιστοίχησης» των πακέτων σε κρυπτοπακέτα. Υπάρχουν και άλλοι τρόποι λειτουργίας, που έχουν ειδικά χαρακτηριστικά για να εξυπηρετούν συγκεκριμένες εφαρμογές. Τέσσερις από αυτούς έχουν τυποποιηθεί [**20**] για να χρησιμοποιούνται με το DES και ο πρώτος είναι αυτός που ήδη αναφέραμε (Σχήμα 5).

Ο δεύτερος τυποποιημένος τρόπος λειτουργίας του DES λέγεται *λειτουργία με αλυσωτή σύνδεση των πακέτων* (cipher block chain mode, CBC mode) και φαίνεται στο Σχήμα 6. Πρόκειται για τροποποίηση της ECB λειτουργίας, ως προς το

[2] Υποθέτουμε ότι το μήκος N είναι πολλαπλάσιο του n· και αυτό δε βλάπτει τη γενικότητα, όπως έχουμε ήδη εξηγήσει.



Σχημα 6. Χρήση του DES με αλυσωτή σύνδεση των πακέτων. Το ένα από τα δύο κομμάτια δείχνει την κρυπτογράφηση (πάνω) και το άλλο την αποκρυπτογράφηση (κάτω).

ότι, πριν το διαβάσει η συνάρτηση κρυπτογράφησης, το πακέτο παθαίνει μια αποκλειστική διάζευξη με το προηγούμενο κρυπτοπακέτο —για το πρώτο από τα πακέτα, p_0, η διάζευξη σχηματίζεται με κάποιο αυθαίρετα προεπιλεγμένο και κοινό για τον πομπό και το δέκτη πακέτο, που το ονομάζουμε iv. Πιο αναλυτικά, η ακολουθία των κρυπτοπακέτων είναι η

$$(\mathrm{CBC_e}) \qquad \begin{aligned} q_1 &= e_k(p_1 \oplus \mathrm{iv}), \\ q_i &= e_k(p_i \oplus q_{i-1}), \qquad \text{για κάθε } i = 2, \ldots, \nu, \end{aligned}$$

και από αυτά παίρνουμε πάλι πίσω τα πακέτα ως εξής:

$$(\mathrm{CBC_d}) \qquad \begin{aligned} p_1 &= d_k(q_1) \oplus \mathrm{iv}, \\ p_i &= d_k(q_i) \oplus q_{i-1}, \qquad \text{για κάθε } i = 2, \ldots, \nu. \end{aligned}$$

2.2. Λειτουργία με ανάδραση. Οι άλλοι δύο τυποποιημένοι τρόποι λειτουργίας έχουν σχεδιαστεί με σκοπό την κρυπτογράφηση πακέτων με μήκος μικρότερο από $n = 64$. Η αφορμή προκύπτει από το γεγονός ότι πολλές φορές το μήνυμα που θέλουμε να κρυπτογραφήσουμε είναι ήδη μια σειρά από πεπερασμένες δυαδικές ακολουθίες σταθερού μήκους, έστω l, μόνο που αυτό το μήκος είναι λιγότερο από 64. Σε κάποιες από αυτές τις περιπτώσεις θέλουμε να μπορούμε να κρυπτογραφήσουμε με αυτές τις ακολουθίες ως στοιχειώδεις μονάδες κρυπτογράφησης και όχι με τις 64-άδες που επιβάλλει το DES. Το πιο χαρακτηριστικό τέτοιο παράδειγμα συμβαίνει όταν το μήνυμα είναι μια ακολουθία από ASCII χαρακτήρες, οπότε $l = 8$.

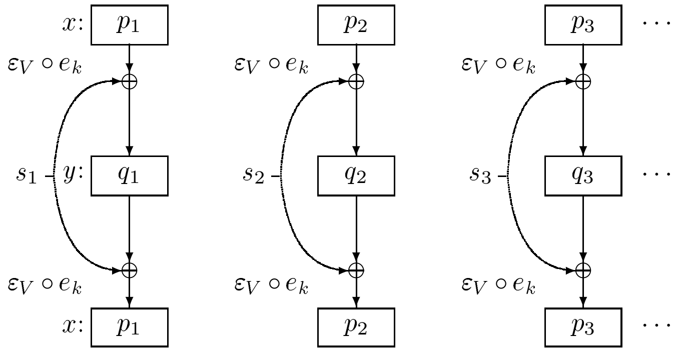
Για ένα μήνυμα λοιπόν που αποτελείται από $\lambda = \frac{N}{l}$ πακέτα μήκους $l \in \{1, \ldots, 64\}$ το καθένα,

$$x = p_1 p_2 \cdots p_\lambda,$$

παραγάγουμε, χρησιμοποιώντας το DES, ένα ρεύμα $(s_i)_{1 \le i \le \lambda}$ από 64-ψήφια πακέτα και κρυπτογραφούμε το μήνυμα σύμφωνα με την εξίσωση

$$(\mathrm{FB_e}) \qquad q_i = p_i \oplus \varepsilon_V\big(e_k(s_i)\big), \qquad \text{για κάθε } i = 1, \ldots, \lambda,$$

όπου $V = [1, 2, \ldots, l]$. Δηλαδή, κάθε φορά κρυπτογραφούμε με το DES το αντίστοιχο πακέτο του ρεύματος και με τα l πιο σημαντικά ψηφία του αποτελέσματος



Σχημα 7. Χρήση του DES με ανάδραση.

εφαρμόζουμε μια διάζευξη στο πακέτο του μηνύματος. Αντίστοιχα, για την αποκρυπτογράφηση ο δέκτης παράγει το ίδιο ρεύμα $(s_i)_{1\leq i\leq\lambda}$ και ανακτά το μήνυμα εκτελώντας την ίδια απλή διάζευξη,

$$(\mathrm{FB_d}) \qquad p_i = q_i \oplus \varepsilon_V\big(e_k(s_i)\big), \qquad \text{για κάθε } i = 1,\dots,\lambda.$$

Το Σχήμα 7 εξηγεί καλύτερα τι συμβαίνει.

Μένει λοιπόν να καθορίσουμε πώς παράγεται το ρεύμα των 64-ψήφιων πακέτων. Θα δείξουμε δύο τρόπους γι' αυτό, κι έτσι θα έχουμε ορίσει τελικά (μαζί και με τα παραπάνω) τους δύο τυποποιημένους τρόπους λειτουργίας που απέμειναν. Σε κάθε περίπτωση το πρώτο πακέτο του ρεύματος είναι μια αυθαίρετα επιλεγμένη τιμή και καθένα από τα επόμενα πακέτα παράγεται από το αμέσως προηγούμενό του μέσω μιας DES κρυπτογράφησης. Αυτό στην πράξη υλοποιείται με μια ανάδραση από την έξοδο στην είσοδο του DES, γι' αυτό και οι αντίστοιχοι τρόποι λειτουργίας λέγονται *λειτουργίες με ανάδραση* (feedback modes, FB modes).

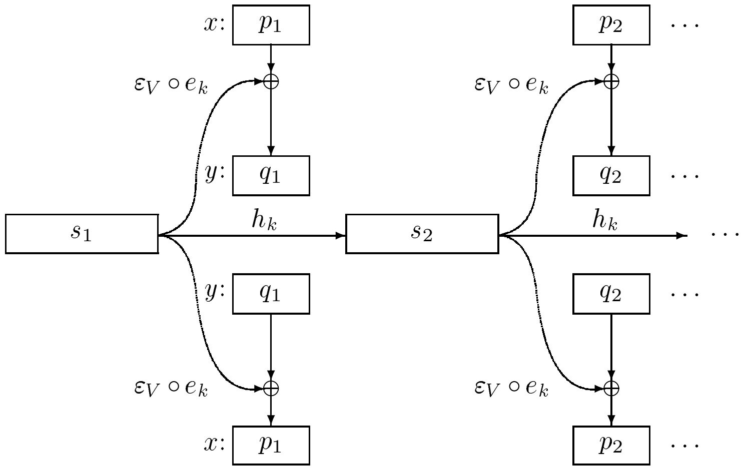
Στη *λειτουργία με ανάδραση από την έξοδο* (output feedback mode, OFB mode), το πρώτο πακέτο s_1 του ρεύματος προκύπτει από μια αυθαίρετα προεπιλεγμένη δυαδική ακολουθία iv μήκους $L \leq 64$, όταν τη συμπληρώσουμε (αν χρειάζεται) με $64 - L$ μηδενικά στις πιο σημαντικές θέσεις. Για να φτιάξουμε καθένα από τα επόμενα πακέτα, s_{i+1}, ολισθαίνουμε το προηγούμενό του, s_i, κατά l θέσεις προς τα αριστερά και τις l λιγότερες σημαντικές θέσεις του, που αδειάζουν, τις αναπληρώνουμε με τα l πιο σημαντικά ψηφία του κρυπτοπακέτου που προκύπτει από την κρυπτογράφηση του s_i. Δηλαδή,

$$(\mathrm{OFB}) \qquad \begin{aligned} s_1 &= 00\cdots0 \,\|\, \mathrm{iv}, \\ s_{i+1} &= \varepsilon_W(s_i) \,\|\, \varepsilon_V\big(e_k(s_i)\big), \qquad \text{για κάθε } i = 2,\dots,\lambda, \end{aligned}$$

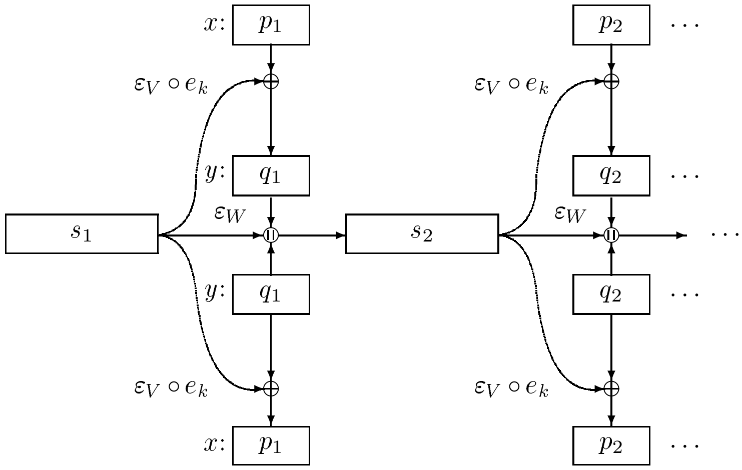
όπου $W = [l+1, l+2, \dots, 64]$ το διάνυσμα για την επιλογή των $64 - l$ λιγότερο σημαντικών ψηφίων.

Στη *λειτουργία με ανάδραση από τα κρυπτοκείμενα* (cipher feedback mode, CFB mode) το πρώτο πακέτο του ρεύματος κατασκευάζεται όπως και στην OFB λειτουργία. Η διαφορά βρίσκεται στην κατασκευή των υπόλοιπων πακέτων, στην οποία συμμετέχουν και τα παραγόμενα l-ψήφια κρυπτοκείμενα, σύμφωνα με τη δεύτερη από τις παρακάτω εξισώσεις:

$$(\mathrm{CFB}) \qquad \begin{aligned} s_1 &= 00\cdots0 \,\|\, \mathrm{iv}, \\ s_{i+1} &= \varepsilon_W(s_i) \,\|\, q_i, \qquad \text{για κάθε } i = 2,\dots,\lambda. \end{aligned}$$



Σχημα 8. Χρήση του DES με ανάδραση από την έξοδο. Όπου $h_k = \| \circ(\varepsilon_W, \varepsilon_V \circ e_k)$.

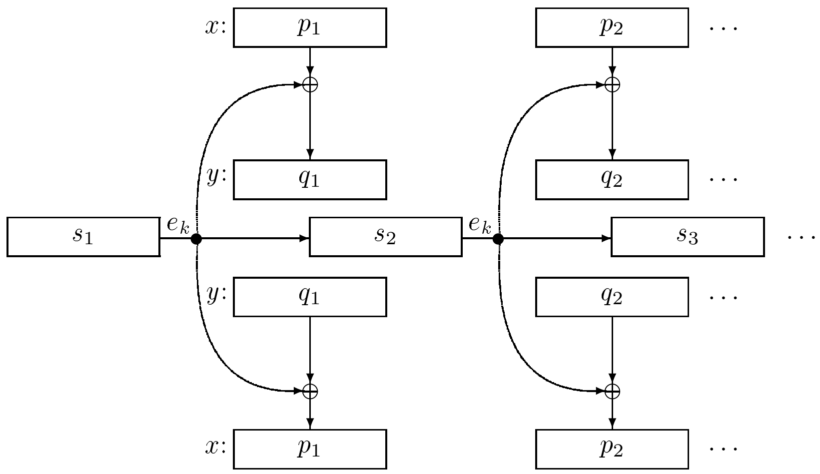


Σχημα 9. Χρήση του DES με ανάδραση από τα κρυπτοκείμενα.

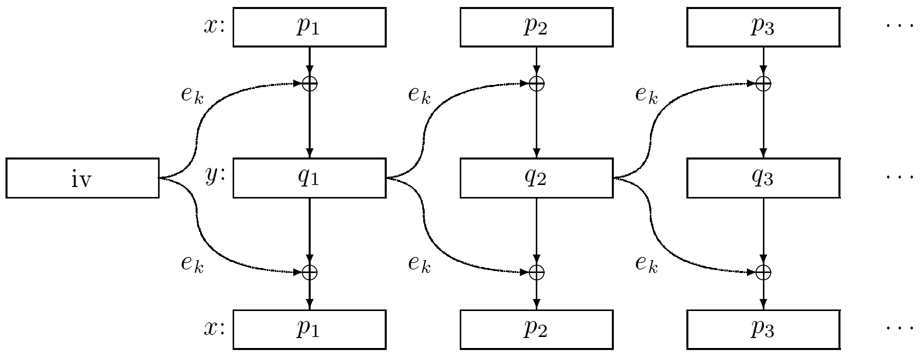
Δηλαδή, για να φτιάξουμε το s_{i+1}, εφαρμόζουμε στο s_i μια αριστερή ολίσθηση κατά l και μετά αναπληρώνουμε τις l λιγότερο σημαντικές θέσεις με το πιο πρόσφατα παραχθέν κρυπτοπακέτο.

Τα Σχήματα 8 και 9 εξηγούν καλύτερα τι συμβαίνει.

Εξάλλου, είναι συχνή και χρήσιμη η εφαρμογή των λειτουργιών ανάδρασης ακόμη και στην περίπτωση που $l = 64$, δηλαδή τα πακέτα στα οποία είναι ήδη χωρισμένο το μήνυμα είναι πράγματι 64-ψήφια. Τότε τα Σχήματα 8 και 9 απλοποιούνται κατά πολύ, και αυτές τις απλοποιημένες εκδοχές δείχνουμε στα Σχήματα 10 και 11.



Σχημα 10. Η λειτουργία με ανάδραση από την έξοδο, όταν $l = 64$.



Σχημα 11. Η λειτουργία με ανάδραση από τα κρυπτοκείμενα, όταν $l = 64$.

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Πινακας 5. Οι 8 πίνακες αντικατάστασης. (Αναπαριστούμε τις τετραψήφιες δυαδικές ακολουθίες με τους αντίστοιχους ακεραίους.)

R_1

9	45	30	53	43	15	29	50	2	8	17	37
3	31	23	22	39	51	52	1	32	24	16	36
20	25	35	48	33	4	42	27	5	47	21	26
54	19	34	56	14	18	40	13	12	55	49	28

R_2

2	38	23	46	36	8	22	43	52	1	10	30
53	24	16	15	32	44	45	51	50	17	9	29
13	18	28	41	26	56	35	20	25	40	14	19
47	12	27	49	7	11	33	6	5	48	42	21

R_3

45	24	9	32	22	51	8	29	38	44	53	16
39	10	2	1	43	30	31	37	36	3	52	15
54	4	14	27	12	42	21	6	11	26	55	5
33	25	13	35	48	56	19	47	18	34	28	7

R_4

31	10	52	43	8	37	51	15	24	30	39	2
50	53	45	44	29	16	17	23	22	46	38	1
40	49	55	13	25	28	7	47	56	12	41	18
19	11	54	21	34	42	5	33	4	20	14	48

R_5

17	53	38	29	51	23	37	1	10	16	50	45
36	39	31	30	15	2	3	9	8	32	24	44
26	35	41	54	11	14	48	33	42	25	27	4
5	56	40	7	20	28	18	19	49	6	55	34

R_6

3	39	24	15	37	9	23	44	53	2	36	31
22	50	17	16	1	45	46	52	51	43	10	30
12	21	27	40	56	55	34	19	28	11	13	49
18	42	26	48	6	14	4	5	35	47	41	20

R_7

46	50	10	1	23	52	9	30	39	45	22	17
8	36	3	2	44	31	32	38	37	29	53	16
25	7	13	26	42	41	20	5	14	56	54	35
4	28	12	34	47	55	49	18	21	33	27	6

R_8

32	36	53	44	9	38	52	16	50	31	8	3
51	22	46	45	30	17	43	24	23	15	39	2
11	48	54	12	28	27	6	18	55	42	40	21
49	14	25	20	33	41	35	4	7	19	13	47

Πίνακας 6. Τα διανύσματα $R_1, \ldots, R_8$.

R_9

50	29	46	37	2	31	45	9	43	24	1	53
44	15	39	38	23	10	36	17	16	8	32	52
4	41	47	5	21	20	54	11	48	35	33	14
42	7	18	13	26	34	28	56	55	12	6	40

R_{10}

36	15	32	23	45	17	31	52	29	10	44	39
30	1	50	24	9	53	22	3	2	51	43	38
49	27	33	18	7	6	40	56	34	21	19	55
28	48	4	54	12	20	14	42	41	25	47	26

R_{11}

22	1	43	9	31	3	17	38	15	53	30	50
16	44	36	10	52	39	8	46	45	37	29	24
35	13	19	4	48	47	26	42	20	7	5	41
14	34	49	40	25	6	55	28	27	11	33	12

R_{12}

8	44	29	52	17	46	3	24	1	39	16	36
2	30	22	53	38	50	51	32	31	23	15	10
21	54	5	49	34	33	12	28	6	48	18	27
55	20	35	26	11	47	41	14	13	56	19	25

R_{13}

51	30	15	38	3	32	46	10	44	50	2	22
45	16	8	39	24	36	37	43	17	9	1	53
7	40	18	35	20	19	25	14	47	34	4	13
41	6	21	12	56	33	27	55	54	42	5	11

R_{14}

37	16	1	24	46	43	32	53	30	36	45	8
31	2	51	50	10	22	23	29	3	52	44	39
48	26	4	21	6	5	11	55	33	20	49	54
27	47	7	25	42	19	13	41	40	28	18	56

R_{15}

23	2	44	10	32	29	43	39	16	22	31	51
17	45	37	36	53	8	9	15	46	38	30	50
34	12	49	7	47	18	56	41	19	6	35	40
13	33	48	11	28	5	54	27	26	14	4	42

R_{16}

16	52	37	3	50	22	36	32	9	15	24	44
10	38	30	29	46	1	2	8	39	31	23	43
27	5	42	55	40	11	49	34	12	54	28	33
6	26	41	4	21	25	47	20	19	7	56	35

ΠΙΝΑΚΑΣ 7. Τα διανύσματα $R_9, \ldots, R_{16}$.

ΚΕΦΑΛΑΙΟ 3

Κρυπτανάλυση

Από τη θέση του σχεδιαστή ενός κρυπτοσυστήματος πακέτου, περνάμε τώρα στη θέση του εχθρού. Θα εξετάσουμε μερικές τεχνικές για να «επιτεθούμε» σε ένα κρυπτοσύστημα. Το σύνολο αυτών των τεχνικών ορίζει την περιοχή της *κρυπτανάλυσης* (cryptanalysis).

Το πρόβλημα είναι να βρούμε μεθόδους που, με *ελάχιστο* δεδομένο ένα από τα κρυπτοκείμενα που έχει στείλει ο πομπός στο δέκτη, θα παραγάγουν κάποια *πληροφορία* για το αντίστοιχο κείμενο και/ή το χρησιμοποιούμενο κλειδί. Αυτή η διατύπωση είναι πολύ γενική και περιλαμβάνει μια σειρά από καταστάσεις στις οποίες είναι δυνατόν να βρισκόμαστε, σε σχέση με το τι ακριβώς γνωρίζουμε και το τι ακριβώς ψάχνουμε να βρούμε.

1. Δεδομένα

Κατ' αρχήν, παραδεχόμαστε μια πολύ βασική γνώση και μια πολύ βασική άγνοια. Η παραδοχή για τη γνώση —την έχουμε ήδη αναφέρει— είναι αυτή του Kerckhoffs. Στην πράξη μπορεί να μην ισχύει, αλλά χωρίς αυτήν δεν μπορούμε να κάνουμε και πολλά πράγματα.

1.1. Παραδοχη. Γνωρίζουμε ποιο κρυπτοσύστημα χρησιμοποιούν ο πομπός και ο δέκτης.

Η παραδοχή για την άγνοια αφορά το κλειδί: δεν έχουμε ιδέα για τον τρόπο με τον οποίον ο πομπός και ο δέκτης έχουν διαλέξει το μυστικό κλειδί. Αυτό στην πράξη μπορεί κάποτε να μην ισχύει,[1] αλλά σίγουρα δεν μπορούμε να υπολογίζουμε σε τέτοια μοιραία λάθη.

1.2. Παραδοχη. Ο πομπός και δέκτης έχουν διαλέξει το κλειδί ομοιόμορφα τυχαία μέσα από το χώρο $\mathcal{K}$ όλων των δυνατών κλειδιών.

Από κει και πέρα, το ασθενέστερο που μπορούμε να υποθέσουμε για τα επιπλέον δεδομένα που έχουμε στη διάθεσή μας προκειμένου να επιτεθούμε σε ένα κρυπτοσύστημα, είναι το ότι έχουμε απλώς κλέψει $N \geq 1$ κρυπτοκείμενα $q_1, \ldots, q_N$ από αυτά που έχει στείλει ο πομπός στο δέκτη.

Πολλές φορές όμως οι γνώσεις μας είναι περισσότερες. Για παράδειγμα, ας υποθέσουμε ότι το Τμήμα Χορηγήσεων κάποιου υποκαταστήματος της Εθνικής Τράπεζας στέλνει κάθε μεσημέρι στην Περιφερειακή του Διοίκηση μια κρυπτογραφημένη με το DES αναφορά με την κίνηση της ημέρας. Ας υποθέσουμε επίσης ότι έχουμε την πληροφορία πως αυτή η αναφορά ξεκινάει πάντα με την τρέχουσα ημερομηνία, στη μορφή

24-7-2000.

[1] Μπορεί, π.χ., να ξέρουμε καλά τον πομπό και να γνωρίζουμε τη συνήθειά του να χρησιμοποιεί σε κωδικούς και κλειδιά ονόματα συγγενικών του προσώπων.

Τότε ξέρουμε τουλάχιστον οχτώ χαρακτήρες από την αρχή του συνολικού μηνύματος, άρα ξέρουμε το πρώτο του πακέτο (υποθέτουμε την ASCII κωδικοποίηση για τους χαρακτήρες). Επομένως, κλέβοντας το πρώτο κρυπτοπακέτο που θα σταλεί ένα μεσημέρι από το συγκεκριμένο υποκατάστημα προς την Περιφερειακή Διοίκηση, ξέρουμε όχι μόνο αυτό το κρυπτοπακέτο, q, αλλά και το πακέτο p από το οποίο προέκυψε. Κάνοντας το ίδιο κάθε εργάσιμη ημέρα του χρόνου, καταλήγουμε να ξέρουμε $N \geq 200$ ζευγάρια $(p_1, q_1), \ldots, (p_N, q_N)$.

Ακόμα και τώρα, μπορούμε να βελτιώσουμε κι άλλο τη θέση μας. Κάποια μέρα καταθέτουμε κι εμείς στο υποκατάστημα μια αίτηση για δάνειο, με την ηλεκτρονική μορφή ενός αρχείου 20 Kilobytes στο MS Word. Είναι βέβαιο ότι η αίτησή μας θα είναι μέρος του μηνύματος που θα σταλεί στην Περιφερειακή Διοίκηση το μεσημέρι. Αν λοιπόν «κρύψουμε» μέσα σ' αυτό το αρχείο μια ακολουθία από 8000 κενά, θα μπορέσουμε το μεσημέρι να ανιχνεύσουμε στο κρυπτογραφημένο μήνυμα μια ακολουθία περίπου 1000 ολόιδιων διαδοχικών κρυπτοκειμένων, καθένα από τα οποία θα είναι η κρυπτογράφηση q του πακέτου p που συνιστούν 8 διαδοχικά κενά. Έτσι, θα έχουμε βρει ένα ζευγάρι (p, q) που το πρώτο του μέλος, το κείμενο p, είναι της δικής μας επιλογής. Εφαρμόζοντας την ίδια τεχνική και με άλλες αιτήσεις και/ή άλλα υποκαταστήματα, μπορούμε τελικά να φτιάξουμε μια ολόκληρη ακολουθία από τέτοια ζευγάρια, διαλέγοντας κάθε φορά κι ένα διαφορετικό κείμενο p. Μάλιστα, εφόσον θέλουμε, η επιλογή του συγκεκριμένου κειμένου μπορεί να γίνεται μόνο εφόσον έχουμε παραγάγει και ξέρουμε όλα τα προηγούμενα ζευγάρια.

Τα παραδείγματα που αναφέραμε καλύπτουν όλο το φάσμα των δυνατοτήτων μας όσον αφορά τις γνώσεις μας κατά την επίθεση (Σχήμα 1).

Επίθεση μόνο με κρυπτοκείμενα (ciphertext only attack): Η περίπτωση κατά την οποία το μόνο που ξέρουμε είναι μια ακολουθία N κρυπτοκειμένων $q_1, \ldots, q_N$ που έχουν σταλεί από τον πομπό στο δέκτη.

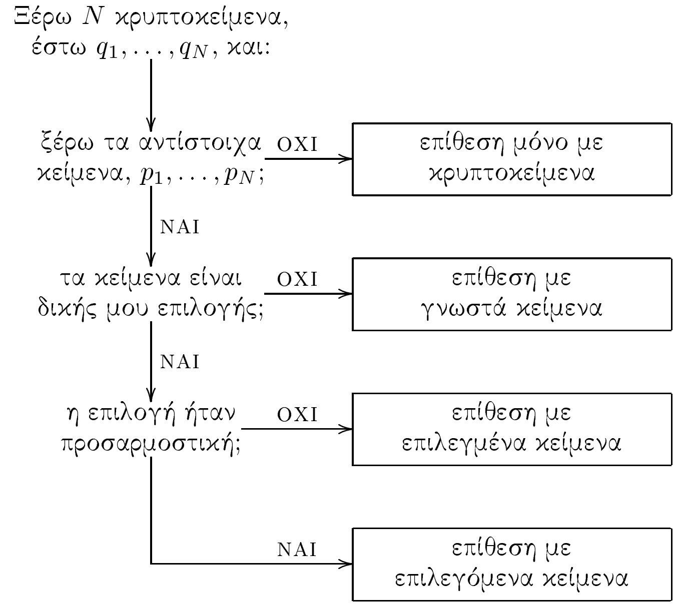
Επίθεση με γνωστά κείμενα (known plaintext attack): Όταν αυτό που γνωρίζουμε είναι μια ακολουθία N ζευγών $(p_1, q_1), \ldots, (p_N, q_N)$ τέτοια που, για κάθε $i = 1, \ldots, N$, το q_i είναι η κρυπτογράφηση του p_i με βάση το χρησιμοποιούμενο κλειδί. Υποθέτουμε ότι δεν έχουμε τη δυνατότητα να διαλέξουμε ποια θα είναι αυτά τα ζευγάρια.

Επίθεση με επιλεγμένα κείμενα (chosen plaintext attack): Όπως η επίθεση με γνωστά κείμενα, με τη διαφορά ότι διαλέξαμε εμείς ποια θα είναι τα $p_1, \ldots, p_N$ και μετά αναγκάσαμε τον πομπό να παραγάγει τα αντίστοιχα κρυποκείμενα.

Επίθεση με επιλεγόμενα κείμενα (adaptively chosen plaintext attack): Σαν την επίθεση με επιλεγμένα κείμενα, με μόνη διαφορά το ότι, για κάθε $i = 1, \ldots, N-1$, είχαμε τη δυνατότητα να διαλέξουμε το p_{i+1} αφού πρώτα μάθαμε το q_i.

Ανάλογα προς τις επιθέσεις με επιλεγμένα και επιλεγόμενα κείμενα, μπορούμε να φανταστούμε την *επίθεση με επιλεγμένα κρυπτοκείμενα* (chosen ciphertext attack) και την *επίθεση με επιλεγόμενα κρυπτοκείμενα* (adaptively chosen ciphertext attack). Αλλά αυτές εφαρμόζονται κυρίως σε κρυπτοσυστήματα δημόσιου κλειδιού και δεν μας απασχολούν εδώ.

Είναι προφανές ότι οι επιθέσεις αναφέρθηκαν κατά γνησίως αύξουσα σειρά ως προς τη δύναμη που κάθε φορά υποθέτουμε ότι έχουμε ως εχθροί. Και όσο πιο ισχυρή είναι η υπόθεση, τόσο πιο δύκολο είναι να ισχύει. Για παράδειγμα, η επίθεση μόνο με



Σχημα 1. Όλες οι δυνατές περιπτώσεις για το ποιες μπορεί να είναι οι γνώσεις μας κατά την επίθεση σε ένα κρυπτοσύστημα.

κρυπτοκείμενα μπορεί να γίνει πάντα, αλλά η επίθεση με επιλεγόμενα κείμενα —όταν είναι δυνατή— είναι κατά κανόνα πολύ πιο χρονοβόρα και ακριβή.

Επιπλέον, το μήκος N της διαθέσιμης ακολουθίας είναι μια πολύ σημαντική παράμετρος για την κάθε επίθεση. Για παράδειγμα, αν ισχύει ότι μπορούμε να κάνουμε μια επίθεση με γνωστά κείμενα για κάποιο $N \to |\mathcal{K}|$, τότε είμαστε πολύ κοντά στο να μπορούμε να κάνουμε και μια επίθεση με N επιλεγμένα (ακόμη και επιλεγόμενα) κείμενα· ώστε η υπόθεση για γνωστά κείμενα γίνεται περίπου ισοδύναμη με αυτήν για επιλεγμένα (ή επιλεγόμενα) κείμενα.

2. Ζητούμενα

Η ισχυρότερη φιλοδοξία που μπορουμε να έχουμε ως εχθροί είναι βεβαίως να βρούμε το μυστικό κλειδί. Όμως υπάρχουν και άλλοι, εξίσου ενδιαφέροντες αν και λιγότερο ισχυροί, τρόποι να βλάψουμε την μυστικότητα της επικοινωνίας πομπού-δέκτη.

Γενικά, η επιτυχία μας μπορεί να είναι μια από τις παρακάτω:

Κατάρρευση του κρυπτοσυστήματος (total break)**:** Είναι η περίπτωση κατά την οποία έχουμε ανακαλύψει το κλειδί. Τότε (λόγω και της Παραδοχής 1.1) μπορούμε να αποκρυπτογραφήσουμε κάθε κρυπτοκείμενο και η μυστικότητα της επικοινωνίας έχει καταρρεύσει.

Καθολική λύση (global deduction)**:** Συμβαίνει όταν, χωρίς να έχουμε ανακαλύψει το κλειδί, έχουμε βρει έναν αλγόριθμο που κάνει την αποκρυπτογράφηση.

Τοπική λύση (instance deduction)**:** Όταν έχουμε ανακαλύψει το κείμενο που αντιστοιχεί σε κάποιο κρυπτοκείμενο και αυτό το κείμενο δεν μας το έδωσε άμεσα κάποιος από τους πομπό-δέκτη.

Απόσπαση πληροφορίας (information deduction)**:** Η περίπτωση κατά την οποία έχουμε εξαγάγει κάποια *πληροφορία* για το κλειδί ή για το κείμενο που αντιστοιχεί σε κάποιο κρυπτοκείμενο και αυτή την πληροφορία δεν την γνωρίζαμε πριν την επίθεση, ούτε μας την έδωσε άμεσα κάποιος από τους πομπό-δέκτη.

Παρατηρήστε ότι η καθολική λύση, αν και ασφαλώς μικρότερη ως επιτυχία από την κατάρρευση, είναι ισοδύναμη με αυτήν όσον αφορά το τελικό αποτέλεσμα: και στις δύο περιπτώσεις μπορούμε να αποκρυπτογραφήσουμε κάθε κρυπτοπακέτο.

Παρόμοια, η τοπική λύση γίνεται ισοδύναμη με την καθολική λύση και την κατάρρευση όταν ο πομπός και ο δέκτης δεν ανταλλάσσουν περισσότερα από ένα κρυπτοκείμενο.

Τέλος, ένα είδος απόσπασης πληροφορίας για το κλειδί (ή το κείμενο που αντιστοιχεί σε κάποιο κρυπτοκείμενο) είναι η ελάττωση του πλήθους των πιθανών του τιμών, που είναι αρχικά $|\mathcal{K}|$ (αντίστοιχα, κάποια τιμή $\leq |\mathcal{P}|$). Όμως η έννοια είναι πιο λεπτή από αυτό και μάλιστα μαθηματική. Την εξηγούμε στην επόμενη ενότητα.

3. Στοιχεία από τη θεωρία του Shannon

Ας είναι Y κάποια άγνωστη ποσότητα, για την οποία ξέρουμε τι τιμές μπορεί να πάρει, έστω $y_1, \ldots, y_b$, και πόσο συχνά συμβαίνει συνήθως να παίρνει καθεμία από αυτές τις τιμές. Έστω ότι ισχύει η ανάλογη υπόθεση για την ποσότητα X και τις τιμές $x_1, \ldots, x_a$. Έστω επίσης ότι, κάθε φορά που μαθαίνουμε την τιμή της Y, αποκτάμε μια καλύτερη ιδέα για το ποια μπορεί να είναι η τιμή της X.[2] Τότε η γνώση της τιμής της Y αυξάνει τη γνώση μας για τη X. Ή, αλλιώς, *ελαττώνει την αβεβαιότητά μας* για την τιμή που έχει τελικά η X.

Θα συζητήσουμε έναν τρόπο για να μαθηματικοποιήσουμε αυτή την διαισθητική έννοια της *ελάττωσης της αβεβαιότητας* για την τιμή μιας ποσότητας. Οι όροι που χρησιμοποιούμε είναι παρμένοι από τη θεωρία του Shannon [**33**], [**34**, Chapter 2]. Και το κίνητρο για τη συζήτηση είναι κρυπτογραφικό: Αν η ποσότητες Y και X είναι αντίστοιχα το πρώτο κρυπτοκείμενο q που στέλνει ο πομπός στο δέκτη και το αντίστοιχο κείμενο p, τότε ασφαλώς έχει νόημα να ρωτάμε πόσο ελαττώνει (αν ελαττώνει) την αβεβαιότητά μας για την τιμή του p η γνώση του q.

Το μαθηματικό μοντέλο για να περιγράψουμε την παραπάνω κατάσταση είναι βεβαίως το πιθανοτικό. Οι ποσότητες Y και X δεν είναι τίποτα περισσότερο από διακριτές τυχαίες μεταβλητές, με γνωστές τις αντίστοιχες συναρτήσεις πιθανότητας, f_Y και f_X.

$$Y = \begin{cases} y_1 & \text{με πιθανότητα } f_Y(y_1) \\ \ldots & \ldots \\ y_b & \text{με πιθανότητα } f_Y(y_b) \end{cases} \qquad X = \begin{cases} x_1 & \text{με πιθανότητα } f_X(x_1) \\ \ldots & \ldots \\ x_a & \text{με πιθανότητα } f_X(x_a). \end{cases}$$

Και ξέρουμε τι σημαίνουν οι συναρτήσεις πιθανότητας $f_{X,Y}$ και $f_{X|y_j}$, για κάθε $j = 1, \ldots, b$.

3.1. Εντροπία. Το πρώτο που κάνουμε είναι να ορίσουμε μια ποσότητα που, δεδομένης μιας διακριτής τυχαίας μεταβλητής με γνωστή συνάρτηση πιθανότητας,

[2] Αυτό συμβαίνει, για παράδειγμα, όταν ξέρουμε κανόνες σαν τον εξής: στην περίπτωση που η τιμή της Y είναι η y_3, τότε το συνηθέστερο που συμβαίνει είναι ότι η X έχει την τιμή x_7, ενώ αποκλείεται να έχει την τιμή x_1, κλπ.

να μετράει την αβεβαιότητα που έχουμε για την τιμή που πρόκειται να πάρει αυτή η μεταβλητή.

3.1. Ορισμος. Έστω X μια διακριτή τυχαία μεταβλητή με τιμές στο σύνολο $\{x_1, \ldots, x_a\}$ και συνάρτηση πιθανότητας f_X. Ονομάζουμε *εντροπία* (entropy) της X την ποσότητα[3]

$$H(X) = -\sum_{i=1}^{a} f_X(x_i) \lg f_X(x_i).$$

Η εντροπία είναι η ποσότητα που ζητάμε. Μια καλή δικαιολογία γι' αυτό είναι το γεγονός ότι η οροφή της, $\lceil H(X) \rceil$, δίνει το μέσο μήκος των δυαδικών αναπαραστάσεων των τιμών $x_1, \ldots, x_a$, όταν η κωδικοποίησή τους έχει επιλεγεί έτσι ώστε να ελαχιστοποιεί το φόρτο ενός ψηφιακού καναλιού που αναλαμβάνει να τα μεταδίδει [**34**, §2.2.1].

Η παρατήρηση που ακολουθεί ενισχύει την εγκυρότητα αυτής της διαισθητικής ερμηνείας.

3.2. Προταση. *Για την τυχαία μεταβλητή X του Ορισμού 3.1,*

$$0 \leq H(X) \leq \lg a$$

και μάλιστα:

(1) *$H(X) = 0$ αν και μόνο αν $a = 1$ —οπότε και $f_X(x_1) = 1$.*
(2) *$H(X) = \lg a$ αν και μόνο αν $f_X(x_i) = \frac{1}{a}$, για κάθε $i = 1, \ldots, a$.*

Αποδειξη. Το κάτω φράγμα και το (1) είναι προφανή. Για το άνω φράγμα και το (2), αρκεί να παρατηρήσουμε ότι τα θετικά ποσά $f_X(x_i)$ $(i = 1, \ldots, a)$ έχουν άθροισμα τη μονάδα και ότι η συνάρτηση $\lg x$ είναι αυστηρά κοίλη στο διάστημα $(0, \infty)$, οπότε από την ανίσωση του Jensen έχουμε ότι

$$\sum_{i=1}^{a} f_X(x_i) \lg \frac{1}{f_X(x_i)} \leq \lg\Big(\sum_{i=1}^{a} f_X(x_i) \frac{1}{f_X(x_i)}\Big) = \lg a,$$

και ότι η ισότητα ισχύει αν και μόνο αν το $f_X(x_i)$ είναι σταθερό, για κάθε $i = 1, \ldots, a$. ⊣

Επομένως, η εντροπία της X γίνεται ελάχιστη όταν η X παίρνει μόνο μία τιμή, οπότε δεν υπάρχει καμία αβεβαιότητα για το ποια θα είναι αυτή. Και γίνεται μέγιστη όταν όλες οι δυνατές τιμές της είναι ισοπίθανες (δηλαδή η X είναι ομοιόμορφα κατανεμημένη), οπότε είναι μέγιστη και η αβεβαιότητα για το ποια από αυτές θα ισχύσει τελικά. Επίσης, μεταξύ ομοιόμορφα κατανεμημένων τυχαίων μεταβλητών, η εντροπία γίνεται μέγιστη για τη μεταβλητή με το μεγαλύτερο πεδίο δυνατών τιμών, άρα και με τη μεγαλύτερη αβεβαιότητα. Ισχύει λοιπόν το σχηματικό συμπέρασμα του Σχήματος 2.

[3] Το άθροισμα είναι καλά ορισμένο μόνο αν $f_X(x_i) > 0$, για κάθε $i = 1, \ldots, a$. Ένας τρόπος για να αποφύγουμε την αοριστία είναι να θεωρήσουμε ότι στο άθροισμα δεν συμμετέχουν όλα τα i, αλλά μόνο εκείνα για τα οποία $f_X(x_i) > 0$. Ο άλλος τρόπος είναι να δεχθούμε ότι $0 \cdot \lg 0 = 0$. Έτσι απλοποιούμε πολύ το συμβολισμό χωρίς να υπάρχει ο κίνδυνος της ασάφειας, αφού σε όσα συζητάμε η ποσότητα $0 \cdot \lg 0$ δεν εμφανίζεται παρά μόνο μέσα σε αθροίσματα που υπολογίζουν την εντροπία.

	$\log a$	
η X ομοιόμορφη	$\uparrow$	πλήρης αβεβαιότητα
εντροπία $H(X)$ της X		αβεβαιότητα για την τιμή της X
η X μονότιμη		πλήρης βεβαιότητα
	0	

Σχημα 2. Η τυχαία μεταβλητή X μπορεί να πάρει συνολικά a το πλήθος διαφορετικές τιμές. Η εντροπία της, $H(X)$, γίνεται ελάχιστη (μηδέν) όταν $a = 1$. Τότε ελαχιστοποιείται (γίνεται μηδενική) και η αβεβαιότητα για την τιμή της μεταβλητής. Αντίστροφα, η εντροπία μεγιστοποιείται ($\lg a$) όταν όλες οι τιμές είναι ισοπίθανες. Ακριβώς τότε είναι μέγιστη και η αβεβαιότητα για την τιμή της. Και, για ισοπίθανες τιμές, η εντροπία αυξάνει με το πλήθος a των τιμών, όπως και η αβεβαιότητα.

3.2. Δεσμευμένη εντροπία. Έστω ότι οι τυχαίες μεταβλητές Y και X δεν είναι ανεξάρτητες. Με γνωστή την τιμή της Y, έστω y_j ($j = 1, \ldots, b$), η συνάρτηση πιθανότητας της X είναι πλέον η $f_{X|y_j}$, με

$$f_{X|y_j}(x_i) = \frac{f_{X,Y}(x_i, y_j)}{f_Y(y_j)},$$

για κάθε $i = 1, \ldots, a$ και κάθε $j = 1, \ldots, b$. Και η εντροπία της X είναι πλέον η

$$H(X|y_j) = -\sum_{i=1}^{a} f_{X|y_j}(x_i) \lg f_{X|y_j}(x_i)$$

και, ανάλογα προς όσα εξηγήσαμε πιο πάνω, είναι ένα μέτρο της αβεβαιότητάς μας για την τιμή της X όταν ξέρουμε ότι $Y = y_j$.

Προφανώς, έχει νόημα να ρωτήσουμε πόση είναι η μέση αβεβαιότητά μας για την τιμή της X δεδομένης της τιμής της Y, όταν η τελευταία αλλάζει τιμές σύμφωνα με την κατανομή της. Πρόκειται βεβαίως για την ποσότητα

$$\begin{aligned} E[H(X|Y)] &= -\sum_{j=1}^{b} f_Y(y_j) H(X|y_j) \\ &= -\sum_{j=1}^{b} f_Y(y_j) \sum_{i=1}^{a} f_{X|y_j}(x_i) \lg f_{X|y_j}(x_i) \\ &= -\sum_{j=1}^{b} \sum_{i=1}^{a} f_Y(y_j) f_{X|y_j}(x_i) \lg f_{X|y_j}(x_i). \end{aligned}$$

3.3. Ορισμος. Έστω X και Y τυχαίες μεταβλητές με τιμές στα $\{x_1, \ldots, x_a\}$ και $\{y_1, \ldots, y_b\}$, και συναρτήσεις πιθανότητας f_X και f_Y, αντίστοιχα. Η *δεσμευμένη εντροπία* (conditional entropy) της X ως προς την Y είναι η ποσότητα

$$H(X|Y) = -\sum_{j=1}^{b} \sum_{i=1}^{a} f_Y(y_j) f_{X|y_j}(x_i) \lg f_{X|y_j}(x_i).$$

Όπως περιμένουμε, η γνώση της τιμής της Y μόνο να ελαττώσει μπορεί την αρχική μας αβεβαιότητα για την τιμή της X. Και δεν το κάνει, αν και μόνο αν οι δύο μεταβλητές είναι ανεξάρτητες.

3.4. Πρόταση. *Για κάθε δύο διακριτές τυχαίες μεταβλητές X και Y, είναι*

$$H(X|Y) \leq H(X),$$

και η ισότητα ισχύει αν και μόνο αν οι μεταβλητές είναι ανεξάρτητες.

Για την απόδειξη χρειαζόμαστε πρώτα κάποια άλλα αποτελέσματα.

3.5. Πρόταση. *Για κάθε δύο τυχαίες μεταβλητές X και Y ισχύει ότι*

$$H(X,Y) = H(Y) + H(X|Y).$$

Απόδειξη. Θεωρούμε τις μεταβλητές του Ορισμού 3.3 και θέτουμε για συντομία $p_{i|j} = f_{X|y_j}(x_i)$, $q_j = f_Y(y_j)$ και $r_{i,j} = f_{X,Y}(x_i, y_j)$. Τότε υπολογίζουμε

$$\begin{aligned}
H(Y) + H(X|Y) &= \sum_{j=1}^{b} q_j \lg \frac{1}{q_j} + \sum_{j=1}^{b} q_j \sum_{i=1}^{a} p_{i|j} \lg \frac{1}{p_{i|j}} \\
&= \sum_{j=1}^{b} q_j \Big[\lg \frac{1}{q_j} + \sum_{i=1}^{a} \frac{r_{i,j}}{q_j} \lg \frac{q_j}{r_{i,j}} \Big] \\
&= \sum_{j=1}^{b} q_j \Big[\lg \frac{1}{q_j} + \sum_{i=1}^{a} \frac{r_{i,j}}{q_j} \lg q_j - \sum_{i=1}^{a} \frac{r_{i,j}}{q_j} \lg r_{i,j} \Big] \\
&= \sum_{j=1}^{b} q_j \Big[\lg \frac{1}{q_j} + \frac{\lg q_j}{q_j} \sum_{i=1}^{a} r_{i,j} - \frac{1}{q_j} \sum_{i=1}^{a} r_{i,j} \lg r_{i,j} \Big] \\
&= \sum_{j=1}^{b} q_j \Big[- \lg q_j + \frac{\lg q_j}{q_j} q_j - \frac{1}{q_j} \sum_{i=1}^{a} r_{i,j} \lg r_{i,j} \Big] \\
&= - \sum_{j=1}^{b} \sum_{i=1}^{a} r_{i,j} \lg r_{i,j}.
\end{aligned}$$

Η τελευταία ποσότητα είναι ακριβώς η εντροπία $H(X,Y)$. ⊣

3.6. Πρόταση. *Για κάθε δύο τυχαίες μεταβλητές X και Y ισχύει ότι*

$$H(X,Y) \leq H(X) + H(Y)$$

και η ισότητα ισχύει αν και μόνο αν οι μεταβλητές είναι ανεξάρτητες.

Απόδειξη. Θεωρούμε και πάλι τις τυχαίες μεταβλητές του Ορισμού 3.3, και για συντομία ονοματίζουμε $p_i = f_X(x_i)$, $q_j = f_Y(y_j)$, $r_{i,j} = f_{X,Y}(x_i, y_j)$. Τότε υπολογίζουμε

$$\begin{aligned}
H(X) + H(Y) &= \sum_{i=1}^{a} p_i \lg \frac{1}{p_i} + \sum_{j=1}^{b} q_j \lg \frac{1}{q_j} \\
&= \sum_{i=1}^{a} \sum_{j=1}^{b} r_{i,j} \lg \frac{1}{p_i} + \sum_{j=1}^{b} \sum_{i=1}^{a} r_{i,j} \lg \frac{1}{q_j}
\end{aligned}$$

$$= \sum_{i=1}^{a}\sum_{j=1}^{b} r_{i,j}\Big[\lg\frac{1}{p_i} + \lg\frac{1}{q_j}\Big]$$
$$= \sum_{i=1}^{a}\sum_{j=1}^{b} r_{i,j}\lg\frac{1}{p_i q_j}.$$

Επομένως, η διαφορά $H(X,Y) - [H(X)+H(Y)]$ είναι η

$$\sum_{i=1}^{a}\sum_{j=1}^{b} r_{i,j}\lg\frac{1}{r_{i,j}} - \sum_{i=1}^{a}\sum_{j=1}^{b} r_{i,j}\lg\frac{1}{p_i q_j}$$
$$= \sum_{i=1}^{a}\sum_{j=1}^{b} r_{i,j}\Big[\lg\frac{1}{r_{i,j}} - \lg\frac{1}{p_i q_j}\Big] = \sum_{i=1}^{a}\sum_{j=1}^{b} r_{i,j}\Big[\lg\frac{p_i q_j}{r_{i,j}}\Big].$$

Αλλά οι ποσότητες $r_{i,j}$ (για όλα τα $i = 1,\ldots,a$ και $j = 1,\ldots,b$) είναι θετικές και αθροίζονται στη μονάδα. Επιπλέον, η συνάρτηση $\lg x$ είναι αυστηρά κοίλη στο $(0,\infty)$, κι έτσι από την ανίσωση Jensen ξέρουμε ότι

$$H(X,Y) - [H(X)+H(Y)] \le \lg\sum_{i=1}^{a}\sum_{j=1}^{b} r_{i,j}\frac{p_i q_j}{r_{i,j}} = \lg\sum_{i=1}^{a}\sum_{j=1}^{b} p_i q_j = \lg 1 = 0,$$

με την ισότητα να ισχύει αν και μόνο αν το πηλίκο $\frac{p_i q_j}{r_{i,j}}$ δεν εξαρτάται από τα i, j. Αλλά αυτό συμβαίνει αν και μόνο αν αυτό το πηλίκο είναι μονάδα και επομένως αν και μόνο αν οι X και Y είναι ανεξάρτητες. ⊣

Απόδειξη της Πρότασης 3.4. Από τις Προτάσεις 3.6 και 3.5 ξέρουμε ότι

$$H(X,Y) \le H(X) + H(Y) \qquad \text{και} \qquad H(X,Y) = H(Y) + H(X|Y),$$

οπότε άμεσα και $H(X|Y) \le H(X)$, με την ισότητα να ισχύει (λόγω της 3.6) αν και μόνο αν οι X, Y είναι ανεξάρτητες. ⊣

3.3. Πληροφορία. Επομένως, η γνώση της Y ελαττώνει την αβεβαιότητά μας για την τιμή της X. Διαισθητικά αυτό σημαίνει ότι μαθαίνοντας την τιμή της Y παίρνουμε κάποια επιπλέον πληροφορία για την τιμή της X. Και είναι φυσικό να διαλέξουμε ως μέτρο αυτής της κερδισμένης πληροφορίας την ελάττωση ακριβώς της αβεβαιότητάς μας για τη X.

3.7. Ορισμος. Έστω X και Y δύο διακριτές τυχαίες μεταβλητές. Λέμε ότι η ποσότητα

$$I(X;Y) = H(X) - H(X|Y)$$

είναι η *πληροφορία* (information) που αποκαλύπτει η Y για τη X.

Και από τις Προτάσεις 3.2 και 3.4 είναι άμεσο το επόμενο πόρισμα.

3.8. Πορισμα. *Για κάθε δύο τυχαίες μεταβλητές X και Y, είναι*

$$0 \le I(X;Y) \le H(X)$$

και μάλιστα:

- *$I(X;Y) = 0$ αν και μόνο αν οι μεταβλητές είναι ανεξάρτητες.*
- *$I(X;Y) = H(X)$ αν και μόνο αν η X είναι αιτιοκρατική συνάρτηση της Y.*

3.4. Θεωρητική ασφάλεια κρυπτοσυστήματος. Τώρα είμαστε έτοιμοι να δώσουμε έναν μαθηματικό ορισμό της έννοιας του *ασφαλούς κρυπτοσυστήματος*.

Βεβαίως, το διαισθητικό νόημα της φράσης «το κρυπτοσύστημα είναι ασφαλές» είναι ότι, χρησιμοποιώντας το κρυπτοσύστημα, ο πομπός και ο δέκτης εξασφαλίζουν τη μυστικότητα της επικοινωνίας τους. Πιο αναλυτικά, αυτό σημαίνει ότι παρά την ελεύθερη πρόσβαση στα κρυπτοκείμενα, ο εχθρός δεν μπορεί να μάθει *τίποτα* για τα αντίστοιχα κείμενα. Ακόμη πιο αναλυτικά: η αβεβαιότητα του εχθρού για το ποιο μπορεί να είναι το τυχόν κείμενο που στέλνει ο πομπός στο δέκτη δεν ελαττώνεται από τη γνώση του αντίστοιχου κρυπτοκείμενου.

Για να μιλήσουμε πιο μαθηματικά, πρέπει πρώτα να πούμε ότι το τυχόν κρυπτοκείμενο που πρόκειται να υποκλαπεί από το κανάλι της επικοινωνίας είναι για τον εχθρό μια τυχαία μεταβλητή, έστω Q, ομοιόμορφα κατανεμημένη μέσα στο χώρο $\mathcal{Q}$ όλων των κρυπτοκειμένων. Και ότι, παρόμοια, το αντίστοιχο κείμενο είναι επίσης μια τυχαία μεταβλητή, έστω P, επίσης ομοιόμορφα κατανεμημένη μέσα στο χώρο $\mathcal{P}$ όλων των κειμένων. Οπότε, αυτό που είπαμε στην προηγούμενη παράγραφο είναι ότι το κρυπτοσύστημα που χρησιμοποιούν ο πομπός και ο δέκτης είναι ασφαλές όταν η αβεβαιότητα του εχθρού για την τιμή της P δεν ελαττώνεται όταν μαθαίνει την τιμή της Q. Ο επόμενος ορισμός λέει ακριβώς αυτό, όμως με την ορολογία των προηγούμενων ενοτήτων.

3.9. Ορισμος. Έστω Q η τυχαία μεταβλητή που περιγράφει το επόμενο κρυπτοκείμενο που θα υποκλέψει ο εχθρός από το κανάλι της επικοινωνίας και P η τυχαία μεταβλητή που περιγράφει το αντίστοιχο κείμενο. Το κρυπτοσύστημα της επικοινωνίας είναι *ασφαλές* αν

$$I(P;Q) = 0,$$

δηλαδή αν η Q αποκαλύπτει μηδενική πληροφορία για την P.

Εναλλακτικά, θα μπορούμε να ισχυριστούμε ότι το κρυπτοσύστημα είναι ασφαλές αν η γνώση της Q δεν αλλάζει την κατανομή της P, δηλαδή αν $f_{P|Q} = f_P$. Είναι μια εύκολη άσκηση να δείξουμε ότι ένας τέτοιος ορισμός της ασφάλειας είναι ισοδύναμος με τον 3.9.

Βεβαίως, με την απαίτηση του 3.9 κανένα από τα κρυπτοσυστήματα που χρησιμοποιούνται στην πράξη δεν είναι ασφαλές. Για το λόγο αυτό ονομάζουμε την ασφάλεια που μόλις περιγράψαμε *θεωρητική*.

3.5. Εντροπία γλώσσας. Η έννοια της εντροπίας μπορεί να επεκταθεί και σε φυσικές γλώσσες, ως εξής:

3.10. Ορισμος. Έστω L μια γλώσσα. Ονομάζουμε *εντροπία* της L την ποσότητα

$$H_L = \lim_{n\to\infty} \frac{H(P_L^n)}{n},$$

όπου P_L^n είναι, για κάθε $n \geq 1$, η τυχαία μεταβλητή που περιγράφει το αποτέλεσμα της επιλογής μιας συμβολοσειράς μήκους n μέσα από τη γλώσσα.

Δηλαδή η εντροπία της L είναι ένα μέτρο της μέσης αβεβαιότητας ανά γράμμα που έχουμε για μια ακολουθία n γραμμάτων, όταν επιλέγουμε αυτήν την ακολουθία μέσα από όλες τις μήκους n ακολουθίες της γλώσσας και το n είναι σημαντικά μεγάλο.

Το ένα ακραίο παράδειγμα είναι η γλώσσα L_1 που έχει μόνο ένα γράμμα στο αλφάβητό της. Τότε υπάρχει μόνο μια ακολουθία n γραμμάτων, για κάθε n, επομένως

$H(P^n) = 0$, και $H_{L_1} = 0$. Στο άλλο άκρο βρίσκεται η εντελώς τυχαία γλώσσα πάνω από ένα αλφάβητο a γραμμάτων, δηλαδή η γλώσσα L_a στην οποία, για κάθε n, όλες οι ακολουθίες n γραμμάτων είναι ισοπίθανες. Τότε η μεταβλητή P^n είναι ομοιόμορφα κατανεμημένη, και $H(P^n) = \lg a^n = n \lg a$, άρα $H_{L_a} = \lg a$.

Όπως φαίνεται κι από τα παραδείγματα, η εντροπία μιας γλώσσας εξαρτάται, ως μέτρο της αβεβαιότητας, από το πλήθος των γραμμάτων στο αλφάβητο της γλώσσας. Όταν δεν θέλουμε να υπάρχει αυτή εξάρτηση, χρησιμοποιούμε ένα άλλο μέτρο της αβεβαιότητας, που βασίζεται στην εντροπία.

3.11. Ορισμος. Έστω L μια γλώσσα πάνω από αλφάβητο a γραμμάτων. Ονομάζουμε *πλεονασμό* (redundancy) της L την ποσότητα

$$R_L = 1 - \frac{H_L}{\lg a}.$$

Καθώς $R_L = \frac{\lg a - H_L}{\lg a} = \frac{H_{L_a} - H_L}{H_{L_a}}$, ο πλεονασμός της L είναι ένα (ανεξάρτητο από το μέγεθος του αλφαβήτου) μέτρο της απόστασης της L από την εντελώς τυχαία γλώσσα με το ίδιο αλφάβητο.

Μετρήσεις για την αγγλική γλώσσα L_e έχουν δώσει εκτιμήσεις ότι $1 \leq H_{L_e} \leq 1.5$, και επομένως ότι $0.68 \leq R_{L_e} \leq 0.79$. Δηλαδή η αγγλική γλώσσα είναι τουλάχιστον 68% λιγότερο τυχαία από την εντελώς τυχαία γλώσσα με 26 γράμματα.

4. Τετριμμένες επιθέσεις

Υπάρχει μια σειρά από επιθέσεις, με διάφορα δεδομένα και ζητούμενα, που μπορούμε εύκολα να σκεφτούμε. Τις παρουσιάζουμε τώρα ξεκινώντας από αυτές που υποθέτουν τη λιγότερες γνώσεις. Θεωρούμε $n = |\mathcal{P}|$ και $m = |\mathcal{Q}|$.

4.1. Απόσπαση πληροφορίας μόνο με κρυπτοκείμενα. Αν είναι $H(P)$ η αβεβαιότητά μας για την τιμή ενός κειμένου, τότε μπορούμε να θεωρούμε ότι μέσα στο χώρο $\mathcal{P}$ όλων των κειμένων υπάρχουν περίπου $2^{H(P)}$ κείμενα με νόημα. Οπότε περίπου τόσα είναι και τα κρυπτοκείμενα που μπορούμε να περιμένουμε.

Αν λοιπόν έχουμε στη διάθεσή μας μια ακολουθία $N \geq 2^{H(P)/2}$ κρυπτοκειμένων $q_1, \ldots, q_N$, τότε από το παράδοξο των γενεθλίων (και υποθέτοντας ότι αυτά τα κρυπτοκείμενα είναι ομοιόμορφα τυχαία διαλεγμένα μέσα από τα κρυπτοκείμενα που προκύπτουν από κείμενα που έχουν νόημα) ξέρουμε ότι είναι πολύ πιθανό δύο από αυτά να ταυτίζονται, δηλαδή να είναι $q_i = q_j$, για κάποια $i, j \in \{1, \ldots, N\}$. Τότε ασφαλώς θα ταυτίζονται και τα αντίστοιχα κείμενα, δηλαδή θα είναι $p_i = p_j$.

Πριν αποκτήσουμε πρόσβαση στα κρυπτοκείμενα και βρούμε δύο που να ταυτίζονται, η πληροφορία που αποκαλύπτει η τυχαία μεταβλητή P_j για την P_i είναι

$$I(P_i; P_j) = H(P_i) - H(P_i|P_j).$$

Αφού διαπιστώσουμε ότι $q_i = q_j$, η P_j καθορίζει πλήρως την P_i, κι έτσι η πληροφορία που μας αποκαλύπτει γι' αυτήν είναι

$$I'(P_i; P_j) = H'(P_i) - H'(P_i|P_j) = H(P_i) - 0 = H(P_i).$$

Επομένως, υποκλέπτοντας τα N κρυπτοκείμενα και βρίσκοντας δύο που να ταυτίζονται, αποσπούμε μη μηδενικό ποσό πληροφορίας,

$$I'(P_i; P_j) - I(P_i; P_j) = H(P_i) - [H(P_i) - H(P_i|P_j)] = H(P_i|P_j) > 0.$$

Προφανώς, η επίθεση απαιτεί τουλάχιστον $2^{H(P)/2}$ κρυπτοκείμενα· στην άσχημη περίπτωση, $H(P) = \lg|\mathcal{P}| = \lg n$ και το συγκεκριμένο πλήθος γίνεται $2^{n/2}$. Βεβαίως, απαιτείται και χρόνος για να εντοπιστούν δύο ίδια κρυπτοκείμενα, ανάλογος του $2^{n/2}$.

4.2. Κατάρρευση μόνο με κρυπτοκείμενα. Δεδομένων N *διαδοχικών* κρυπτοκειμένων $q_1, \ldots, q_N$, παράγουμε για κάθε δυνατό κλειδί $k \in \mathcal{K}$ την ακολουθία $p_1^k, \ldots, p_N^k$ των αντίστοιχων κειμένων και ελέγχουμε αν αυτή αποτελεί ή όχι ένα μήνυμα με νόημα. Αν ναι, τότε το k *ίσως* είναι το σωστό κλειδί. Αν όχι, τότε το k απορρίπτεται.

Έστω ότι στο τέλος, μετά τη δοκιμή όλων των κλειδιών, έχουν μείνει $\lambda \geq 1$ κλειδιά που δεν έχουν απορριφθεί. Αν $\lambda = 1$, τότε το μοναδικό αυτό κλειδί είναι και το σωστό. Όμως είναι δυνατόν να είναι και $\lambda \geq 2$. Δηλαδή είναι πιθανόν περισσότερα από ένα κλειδιά να αποκρυπτογραφούν την αρχική ακολουθία κρυπτοκειμένων σε μια ακολουθία κειμένων με νόημα.[4] Τότε μόνο το ένα από αυτά είναι το σωστό, ενώ τα υπόλοιπα $\lambda - 1$ είναι, όπως λέμε, *παραπλανητικά* (spurious). Και δεν έχουμε τρόπο να τα ξεχωρίσουμε.

Όμως, στην περίπτωση που η γλώσσα από την οποία αντλούνται οι ακολουθίες των κειμένων απέχει αρκετά από την εντελώς τυχαία (δηλαδή έχει μικρή εντροπία) και το κρυπτοσύστημα απέχει αρκετά από το να είναι σταθερό (Σημείωση 4), περιμένουμε διαισθητικά να ισχύει ότι όσο πιο μεγάλη είναι η ακολουθία των κρυπτοκειμένων τόσο πιο δύσκολο είναι για ένα κλειδί που δεν είναι το σωστό να αντιστοιχήσει αυτή την ακολουθία σε μια ακολουθία κειμένων που να έχει νόημα.

Ξεκινώντας από αυτή η διαισθητική παρατήρηση, μπορούμε να υπολογίσουμε ένα κάτω φράγμα για την αναμενόμενη τιμή του πλήθους των παραπλανητικών κλειδιών που μπορούν να υπάρχουν για μια τυχαία ακολουθία κρυπτοκειμένων.

4.1. Λημμα. *Έστω $(\mathcal{P}, \mathcal{Q}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ένα κρυπτοσύστημα με κείμενα από μια γλώσσα με πλεονασμό R και με $|\mathcal{P}| = |\mathcal{Q}|$. Για κάθε αρκετά μεγάλο $N \geq 1$, η αναμενόμενη τιμή του πλήθους s_N των παραπλανητικών κλειδιών που αντιστοιχούν σε μια τυχαία ακολουθία N κρυπτοκειμένων είναι τέτοια ώστε*

$$\overline{s_N} \geq \frac{|\mathcal{K}|}{|\mathcal{P}|^{NR}} - 1.$$

Αποδειξη. Ξεκινάμε από το τυχαίο πείραμα της επιλογής N κρυπτοκειμένων μέσα από τον αντίστοιχο χώρο $\mathcal{Q}$. Ονομάζουμε $\bar{Q}$ την τυχαία μεταβλητή που περιγράφει το αποτέλεσμα του πειράματος. Για κάθε τιμή $\bar{q}$ της $\bar{Q}$ ορίζεται το πλήθος λ_N των κλειδιών που αποκρυπτογραφούν την $\bar{q}$ σε μια ακολουθία κειμένων $\bar{p}$ που έχει νόημα. Τότε το πλήθος των παραπλανητικών κλειδιών είναι το

$$s_N = \lambda_N - 1$$

και βέβαια είναι μια τυχαία μεταβλητή, συνάρτηση της $\bar{Q}$. Για τη μέση της τιμή μπορούμε να υπολογίσουμε ότι

$$\overline{s_N} = \sum_{\bar{q} \in \mathcal{Q}^N} f_{\bar{Q}}(\bar{q}) s_N = \sum_{\bar{q} \in \mathcal{Q}^N} f_{\bar{Q}}(\bar{q})(\lambda_N - 1)$$

[4] Αυτό καθόλου δεν αποκλείεται να συμβεί. Μάλιστα, η ακραία περίπτωση είναι αυτή ενός *σταθερού κρυπτοσυστήματος*, που ορίζει πάντα την ίδια αντιστοιχία $e_k : \mathcal{P} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathcal{Q}$, για κάθε $k \in \mathcal{K}$. Τότε, κάθε φορά που θα δοκιμάζουμε την παραπάνω τεχνική, θα καταλήγουμε σε $|\mathcal{K}|$ υποψήφια κλειδιά, ώστε η όποια αξία της επίθεσης που περιγράψαμε ακυρώνεται. Βεβαίως, ένα τέτοιο κρυπτοσύστημα μπορεί να υποκύψει πολύ εύκολα σε άλλου είδους επιθέσεις και γι' αυτό η αναφορά του εδώ έχει μόνο την αξία ενός θεωρητικού παραδείγματος.

$$= \sum_{\bar{q}\in\mathcal{Q}^N} f_{\bar{Q}}(\bar{q})\lambda_N - \sum_{\bar{q}\in\mathcal{Q}^N} f_{\bar{Q}}(\bar{q}) = \Big[\sum_{\bar{q}\in\mathcal{Q}^N} f_{\bar{Q}}(\bar{q})\lambda_N\Big] - 1,$$

και επομένως ότι

$$\overline{s_N} + 1 = \sum_{\bar{q}\in\mathcal{Q}^N} f_{\bar{Q}}(\bar{q})\lambda_N. \tag{1}$$

Τώρα μπορούμε να συνδέσουμε αυτήν την τιμή με τη δεσμευμένη εντροπία του κλειδιού δεδομένης της ακολουθίας των κρυπτοκειμένων:

$$\begin{aligned} H(K|\bar{Q}) &= \sum_{\bar{q}\in\mathcal{Q}^N} f_{\bar{Q}}(\bar{q})H(K|\bar{q}) \\ &\le \sum_{\bar{q}\in\mathcal{Q}^N} f_{\bar{Q}}(\bar{q})\lg\lambda_N \qquad &&(\text{Πρόταση } 3.2) \\ &\le \lg\Big[\sum_{\bar{q}\in\mathcal{Q}^N} f_{\bar{Q}}(\bar{q})\lambda_N\Big] &&(\text{ανίσωση Jensen}) \\ &\le \lg(\overline{s_N}+1), &&(\text{Εξίσωση } (1)) \end{aligned}$$

άρα και

$$\overline{s_N} \ge 2^{H(K|\bar{Q})} - 1. \tag{2}$$

Για να υπολογίσουμε την εντροπία $H(K|\bar{Q})$, ξεκινάμε από την Πρόταση 3.5 και παρατηρούμε ότι $H(K|\bar{Q}) = H(K,\bar{Q}) - H(\bar{Q})$. Αλλά, από την ίδια πρόταση,

$$H(K,\bar{Q}) = H(K,\bar{P},\bar{Q}) - H(\bar{P}|K,\bar{Q}) = H(K,\bar{P},\bar{Q}),$$

αφού $H(\bar{P}|K,\bar{Q}) = 0$, γιατί η γνώση των K και $\bar{Q}$ καθορίζει πλήρως την $\bar{P}$. Παρόμοια, ισχύει ότι

$$H(K,\bar{P}) = H(K,\bar{P},\bar{Q}) - H(\bar{Q}|K,\bar{P}) = H(K,\bar{P},\bar{Q}),$$

κι έτσι έχουμε $H(K,\bar{Q}) = H(K,\bar{P})$. Αλλά $H(K,\bar{P}) = H(K) + H(\bar{P})$, γιατί τα K και $\bar{P}$ είναι ανεξάρτητα. Άρα και $H(K,\bar{Q}) = H(K) + H(\bar{P})$. Τελικά,

$$H(K|\bar{Q}) = H(K) + H(\bar{P}) - H(\bar{Q}). \tag{3}$$

Τώρα παρατηρούμε ότι το κλειδί είναι ομοιόμορφα διαλεγμένο μέσα από το χώρο $\mathcal{K}$, οπότε $H(K) = \lg|\mathcal{K}|$. Εξάλλου, από την Πρόταση 3.2, είναι $H(\bar{Q}) \le \lg|\mathcal{Q}^N| = N\lg|\mathcal{Q}|$. Και, αν το N είναι αρκετά μεγάλο, είναι καλή η προσέγγιση

$$H_L \approx \frac{H(\bar{P})}{N} \Longrightarrow H(\bar{P}) \approx NH_L = N(1-R_L)\lg|\mathcal{P}|.$$

Τελικά, από την Εξίσωση (3) προκύπτει ότι

$$H(K|\bar{Q}) \ge \lg|\mathcal{K}| + N(1-R_L)\lg|\mathcal{P}| - N\lg|\mathcal{Q}|.$$

Κι αφού $|\mathcal{P}| = |\mathcal{Q}|$, έπεται ότι

$$H(K|\bar{Q}) \ge \lg|\mathcal{K}| - NR_L\lg|\mathcal{P}|. \tag{4}$$

Τελικά οι (2) και (4) δίνουν τη ζητούμενη ανίσωση. ⊣

Η χρησιμότητα αυτού του υπολογισμού έγκειται στο ότι τώρα μπορούμε να υπολογίσουμε άμεσα ένα κάτω φράγμα για το πόσο μεγάλη πρέπει να είναι η ακολουθία των κρυπτοκειμένων στην οποία θα βασίσουμε την επίθεσή μας, αν θέλουμε να περιμένουμε ότι δεν πρόκειται να εμφανιστούν παραπλανητικά κλειδιά. Αυτό που περιγράφουμε έχει συγκεκριμένο όνομα.

4.2. Ορισμος. Ονομάζουμε unicity distance N_u ενός κρυπτοσυστήματος το ελάχιστο μήκος που πρέπει να έχει μια ακολουθία κρυπτοκειμένων, για να *περιμένουμε* ότι το πλήθος των παραπλανητικών κλειδιών που αντιστοιχούν σ' αυτή είναι 0.

4.3. Πορισμα. *Η ελάχιστη τιμή για την unicity distance N_u του κρυπτοσυστήματος του Λήμματος* 4.1 *είναι η*

$$N_0 = \left\lceil \frac{\lg |K|}{R \lg |\mathcal{P}|} \right\rceil. \tag{5}$$

Αποδειξη. Άμεσα, από το Λήμμα 4.1. ⊣

Είναι σημαντικό να παρατηρήσουμε ότι η τιμή N_0 είναι απλά ένα κάτω φράγμα για την N_u και όχι μια εκτίμησή της. Το ακραίο αντιπαράδειγμα είναι και πάλι το τυχόν σταθερό κρυπτοσύστημα (Σημείωση 4), όπου το πλήθος των παραπλανητικών κλειδιών είναι πάντα $s_N = |\mathcal{K}| - 1$, για κάθε N, κι επομένως η μέση τιμή του δεν μπορεί να γίνει ποτέ 0, όσο μεγάλο κι αν γίνει το N. Άρα $N_u = \infty$.

Τελικά, η επίθεση που περιγράψαμε χρειάζεται τουλάχιστον N_0 διαδοχικά κρυπτοκείμενα και χρόνο $O(2^m)$, ενώ δεν απαιτεί περισσότερο από σταθερό χώρο. Όμως δεν εξασφαλίζει την εύρεση του κλειδιού.

4.3. Τοπική λύση με γνωστά κείμενα. Δεδομένων $N = |\mathcal{P}| - 1$ ζευγαριών $(p_1, q_1), \ldots, (p_N, q_N)$, το κρυπτοκείμενο που λείπει (δηλαδή αυτό που δεν εμφανίζεται σε κανένα από τα δεύτερα μέλη) είναι (εύκολα) το

$$q_{N+1} = \bigoplus_{i=1}^{N} q_i$$

και, επειδή η e_k είναι αντιστοιχία, η αποκρυπτογράφησή του είναι το κείμενο που λείπει (δηλαδή αυτό που δεν εμφανίζεται σε κανένα από τα πρώτα μέλη). Εύκολα, πρόκειται για το

$$p_{N+1} = \bigoplus_{i=1}^{N} p_i.$$

Επομένως, ο αλγόριθμος που περιγράφουμε δεν απαιτεί προεπεξεργασία, αλλά χρειάζεται $O(2^n)$ ζευγάρια στην είσοδο, $O(2^n)$ χρόνο και σταθερό χώρο.

4.4. Κατάρρευση με γνωστά κείμενα. Δεδομένης μιας ακολουθίας N ζευγών $(p_1, q_1), \ldots, (p_N, q_N)$, ελέγχουμε για κάθε κλειδί $k \in \mathcal{K}$ αν η αποκρυπτογράφηση $p_1^k, \ldots, p_N^k$ της ακολουθίας $q_1, \ldots, q_N$ είναι η ακολουθία $p_1, \ldots, p_N$. Κάθε φορά που ο έλεγχος αποτυγχάνει το k απορρίπτεται. Τελικά θα απομείνουν $\lambda \geq 1$ κλειδιά· μόνο ένα από αυτά είναι το σωστό, ενώ τα υπόλοιπα $\lambda - 1$ είναι παραλανητικά.

Η μέθοδος είναι παρόμοια με τη μέθοδο που περιγράψαμε για την κατάρρευση με μόνο κρυπτοκείμενα, με τη διαφορά ότι εδώ ξέρουμε τη σωστή αποκρυπτογράφηση της ακολουθίας των κρυπτοκειμένων. Προφανώς, τώρα είναι πολύ πιο δύσκολο να εμφανιστούν παραπλανητικά κλειδιά, όμως και πάλι όχι απίθανο. Και, εξασφαλίζοντας ότι $N \geq N_0$ και ότι τα κρυπτοκείμενα είναι διαδοχικά, αυξάνουμε αυτή τη δυσκολία.

Έτσι, η μέθοδος απαιτεί τουλάχιστον N_0 διαδοχικά κρυπτοκείμενα, χρόνο $O(2^m)$ και χώρο σταθερό, αλλά και πάλι δεν εγγυάται την εύρεση του κλειδιού.

4.5. Ολική λύση με επιλεγμένα κείμενα. Δεδομένων όλων των $N = |\mathcal{P}|$ ζευγαριών της μορφής $(p, q) = (p, e_k(q))$, όπου k το χρησιμοποιούμενο κλειδί, ο αλγόριθμος απλά αποθηκεύει αυτά τα ζευγάρια σε έναν $|P| \times 2$ πίνακα και τον ταξινομεί ως προς τη στήλη των κρυπτοκειμένων. Στη συνέχεια, δεδομένου τυχόντος κρυπτοκειμένου q, βρίσκει με μια προσπέλαση στον πίνακα τη μοναδική γραμμή στην οποία εμφανίζεται το q και επιστρέφει το αντίστοιχο κείμενο.

Προφανώς, η προεπεξεργασία απαιτεί χρόνο $O(2^n \lg 2^n) = O(2^n)$, χώρο $O(2^n)$, και $N = 2^n$ ζευγάρια ως δεδομένα στην είσοδο. Ακολούθως, η αποκρυπτογράφηση τυχόντος κρυπτοκειμένου γίνεται σε σταθερό χρόνο.

4.6. Κατάρρευση με επιλεγμένα κείμενα. Σταθεροποιούμε ένα κείμενο $p_0 \in \mathcal{P}$ και το κρυπτογραφούμε με όλα τα κλειδιά, παράγοντας έναν $|\mathcal{K}| \times 2$ πίνακα που

- στην πρώτη στήλη κάθε γραμμής περιέχει και ένα διαφορετικό κλειδί, και
- στη δεύτερη στήλη κάθε γραμμής περιέχει την κρυπτογράφηση του p_0 με βάση το κλειδί της πρώτης στήλης της γραμμής αυτής.

Στη συνέχεια ταξινομούμε τον πίνακα ως προς τη δεύτερη στήλη του. Έτσι, δεδομένου τυχόντος κρυπτοκειμένου q, μπορούμε με μια δυαδική αναζήτηση στην δεύτερη στήλη να βρούμε όλα τα κλειδιά k (αν υπάρχουν) για τα οποία $q = e_k(p_0)$.

Για να καταρρεύσει λοιπόν το κρυπτοσύστημα, αρκεί να βρούμε το κρυπτοκείμενο που αντιστοιχεί στο κείμενο p_0. Βεβαίως, υπάρχει και πάλι το ενδεχόμενο ύπαρξης παραπλανητικών κλειδιών. Για να δυσκολέψουμε την εμφάνισή τους, μπορούμε να φτιάξουμε $t > 1$ πίνακες, για ισάριθμα κείμενα $p_0, \ldots, p_t$, αυξάνοντας το κόστος της μεθόδου κατά ένα σταθερό μόνο παράγοντα.

Προφανώς, η μέθοδος απαιτεί προεπεξεργασία χρόνου $O\big(t \cdot (2^m + 2^m \lg 2^m)\big) = O(t \cdot 2^m)$ και χώρο $O(t \cdot 2^m)$. Στη συνέχεια, το κρυπτοσύστημα καταρρέει με t ζευγάρια $(p_0, q_0), \ldots, (p_t, q_t)$ στα δεδομένα και σε χρόνο $O(t \cdot \lg 2^m) = O(tm)$.

5. Πρακτική ασφάλεια κρυπτοσυστήματος

Από τη συζήτηση της προηγούμενης ενότητας πρέπει να έχει ήδη γίνει σαφές ότι το κόστος μας, ως εχθρών, για την εφαρμογή μιας επίθεσης έχει τέσσερις βασικές συνιστώσες:

- το χρόνο προεπεξεργασίας, C_p,
- το πλήθος των δεδομένων για την εκτέλεση μιας επίθεσης, C_d,
- το χρόνο για την εκτέλεση μιας επίθεσης, C_t, και
- το χώρο για την εκτέλεση μιας επίθεσης, C_s.

Από αυτές αποφασίζουμε να αγνοήσουμε την πρώτη, υποθέτοντας ότι τις περισσότερες φορές μπορούμε να βρούμε το χρόνο να προετοιμαστούμε για μια επίθεση. Επίσης, για τις υπόλοιπες συνιστώσες, υποθέτουμε ότι έχουν το ίδιο βάρος.

Με αυτές τις παραδοχές, έχει νόημα να ονομάσουμε κόστος μιας επίθεσης τη μέγιστη από τις τρεις συνιστώσες που μας ενδιαφέρουν.

5.1. Ορισμός. Ονομάζουμε *κόστος* μιας επίθεσης την τιμή

$$C_a = \max(C_d, C_t, C_s).$$

Ο Πίνακας 1 συνοψίζει τις διαπιστώσεις μας για την κάθε συνιστώσα στην καθεμιά από τις τετριμμένες επιθέσεις που περιγράψαμε και δείχνει τα αντίστοιχα κόστη. Η σημαντική παρατήρηση είναι ότι το κόστος δεν πέφτει ποτέ κάτω από $2^{n/2}$.

Τώρα προσπαθούμε να βρούμε έναν ορισμό για την πρακτική ασφάλεια ενός κρυπτοσυστήματος πακέτου. Η πρώτη σκέψη προς αυτή την κατεύθυνση είναι ότι,

Επίθεση	Κόστος			
	Δεδομένα	Χώρος	Χρόνος	Προετοιμασία
απόσπαση πληροφορίας μόνο με κρυπτοκείμενα	$2^{H(P)/2}$	–	$2^{H(P)/2}$	–
κατάρρευση μόνο με κρυπτοκείμενα	$\geq \frac{m}{nR_L}$	–	2^m	–
τοπική λύση με γνωστά κείμενα	2^n	–	2^n	–
κατάρρευση με γνωστά κείμενα	$\geq \frac{m}{nR_L}$	–	2^m	–
ολική λύση με επιλεγμένα κείμενα	2^n	2^n	–	2^n
κατάρρευση με επιλεγμένα κείμενα	–	2^m	m	2^m

Πίνακας 1

για να θεωρηθεί ασφαλές, ένα τέτοιο κρυπτοσύστημα πρέπει πρώτα απ' όλα να καθιστά απαγορευτικό το κόστος καθεμιάς από τις τετριμμένες επιθέσεις. Η δεύτερη σκέψη είναι ότι θα πρέπει και κάθε άλλη γνωστή επίθεση να έχει τη μοίρα των τετριμμένων, δηλαδή να έχει κόστος συγκρίσιμο με το κόστος της φθηνότερης από αυτές. Και η τρίτη σκέψη είναι ότι το περισσότερο που μπορούμε να υποθέσουμε για τα δεδομένα της επίθεσης είναι ότι αυτή γίνεται με επιλεγόμενα κείμενα, ενώ το λιγότερο που μπορούμε να υποθέσουμε για τα αποτελέσματά της είναι η απόσπαση πληροφορίας.

5.2. Ορισμος. Λέμε ότι ένα κρυπτοσύστημα πακέτου με διαστάσεις $n \times m$ είναι *πρακτικά ασφαλές* (practically secure) αν κάθε γνωστή εναντίον του επίθεση με επιλεγόμενα κείμενα με σκοπό την απόσπαση πληροφορίας έχει κόστος συγκρίσιμο με $2^{n/2}$.

ΚΕΦΑΛΑΙΟ 4

Διαφορική κρυπτανάλυση

Η *διαφορική κρυπτανάλυση* (differential cryptanalysis) είναι μια επίθεση με επιλεγμένα κείμενα που πρωτοεφαρμόστηκε στο DES [**2, 3, 4**] με σημαντική επιτυχία: ήταν η πρώτη που μπόρεσε να πετύχει την κατάρρευση του συγκεκριμένου κρυπτοσυστήματος σε χρόνο μικρότερο από αυτό της εξαντλητικής αναζήτησης.[1] Στη συνέχεια εφαρμόστηκε και σε πολλά άλλα κρυπτοσυστήματα πακέτου με εξίσου σημαντικά, αν όχι καλύτερα, αποτελέσματα.

1. Συμβάσεις–συμβολισμοί

Στην ενότητα αυτή εξηγούμε την τεχνική πάνω στο DES.

Υποθέτουμε σταθερά ότι το κλειδί που χρησιμοποιούν ο πομπός και ο δέκτης είναι κάποιο (άγνωστο σε μας, αλλά) σταθερό $k \in \mathbb{B}^{56}$. Και για να κάνουμε την ανάλυση πιο ευέλικτη, θεωρούμε ότι το Feistel δίκτυο της συνάρτησης κρυπτογράφησης έχει $r \in \{2, 3, \ldots, 16\}$ γύρους, όπου το r είναι βέβαια σταθερό, αλλά όχι απαραίτητα 16. Έτσι, το υποκλειδί για τον τελευταίο γύρο του δικτύου είναι το $\varepsilon_{R_r}(k)$. Το συμβολίζουμε σταθερά με u.

Εξάλλου, παρατηρούμε ότι, για κάθε γνωστό ζευγάρι (p, q) κειμένου-κρυπτοκειμένου, μπορούμε άμεσα να βρούμε το ζευγάρι $\big(\varepsilon_{\mathrm{IP}}(p), (\circlearrowleft \circ \varepsilon_{\mathrm{IP}})(q)\big)$, δηλαδή την είσοδο και την έξοδο της σύνθεσης των r Feistel γύρων της συνάρτησης κρυπτογράφησης. Επομένως, τουλάχιστον για επιθέσεις με γνωστά κείμενα (άρα και για την επίθεση με επιλεγμένα κείμενα που πρόκειται να εξετάσουμε), οι μεταθέσεις $\varepsilon_{\mathrm{IP}}$ και $\varepsilon_{\mathrm{IP}^{-1}} \circ \circlearrowleft$ δεν προσφέρουν καθόλου στην ασφάλεια του DES. Μπορούμε λοιπόν, για απλότητα, να τις αγνοήσουμε και να επιτεθούμε μόνο στη σύνθεση των Feistel γύρων. Θεωρούμε δηλαδή για τη συνέχεια ότι η συνάρτηση κρυπτογράφησης του DES είναι μόνο η

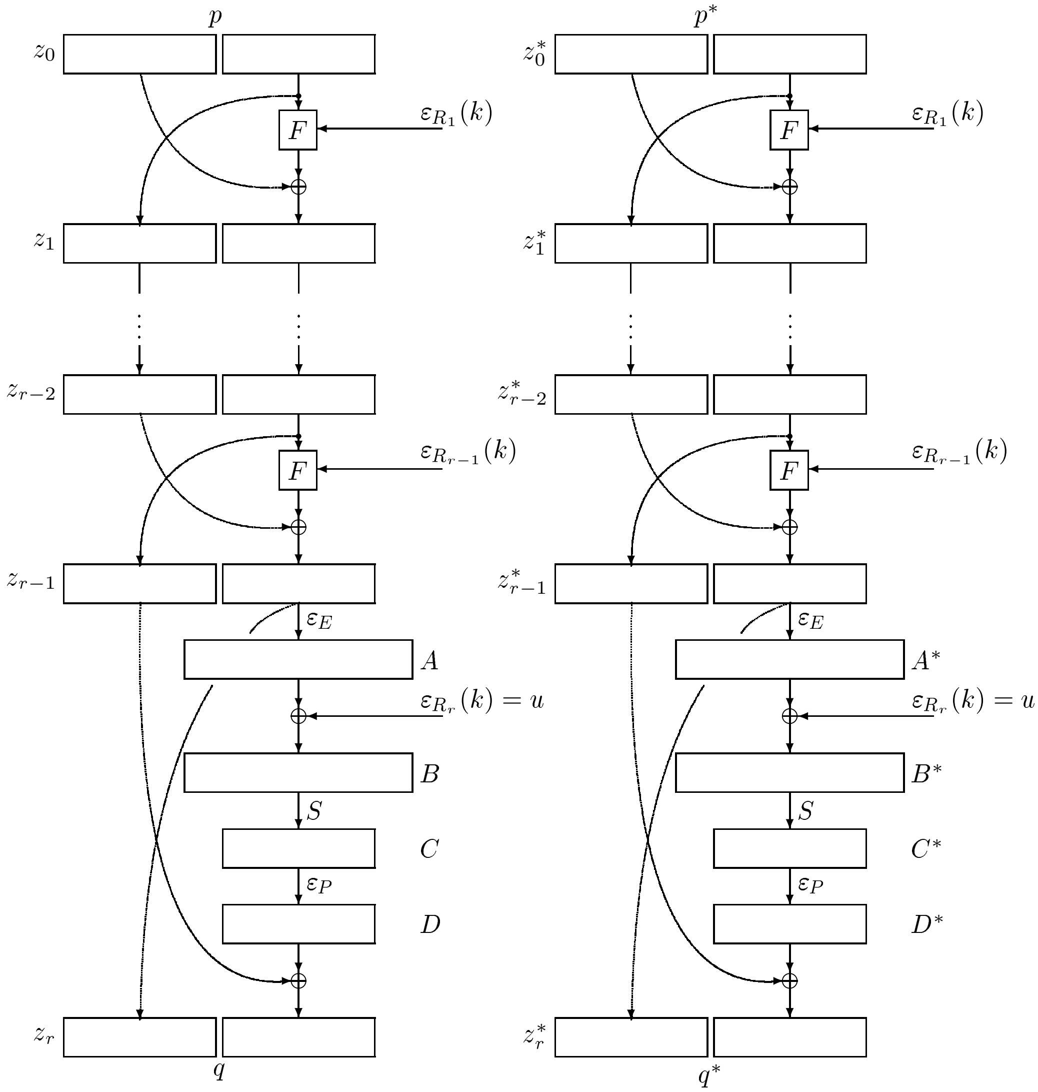
$$e_k = f_u \circ f_{\varepsilon_{R_{r-1}}(k)} \circ \cdots \circ f_{\varepsilon_{R_1}(k)}, \tag{1}$$

όπου f_v η Feistel μετάθεση πάνω από τη συνάρτηση F του DES που ορίζεται από το υποκλειδί $v \in \mathbb{B}^{48}$.

Για να εξηγήσουμε τη συλλογιστική της επίθεσης, θα δουλέψουμε με δύο κρυπτοκείμενα, που θα τα συμβολίζουμε σταθερά με q και q^*. Θα χρειαστούμε επίσης σταθερά σύμβολα για όλες τις σχετικές με το κάθε κρυπτοκείμενο ποσότητες (Σχήμα 1). Έτσι, p θα είναι το κείμενο που αντιστοιχεί στο q, ώστε $q = e_k(p)$. Και

$$\begin{aligned} z_0 &= p \\ z_i &= f_{\varepsilon_{R_i}(k)}(z_{i-1}) \qquad (1 \le i \le r) \end{aligned}$$

[1]Αν και, για τη σύγκριση αυτή, δεν πρέπει να ξεχνάμε ότι η εξαντλητική αναζήτηση είναι μια επίθεση με μόνο κρυπτοκείμενα, ή με γνωστά κείμενα —σε κάθε περίπτωση η υποθέση για τις γνώσεις του εχθρού είναι ασθενέστερη από αυτήν των επιλεγμένων κειμένων.



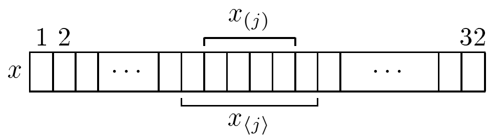
Σχημα 1. Κρυπτογράφηση δύο πακέτων, των p και p^*. Στον τελευταίο γύρο δείχνουμε αναλυτικά τις πράξεις για τον υπολογισμό της συνάρτησης F.

θα είναι όλα τα ενδιάμεσα πακέτα που υπολογίζονται μέχρι να παραχθεί τελικά το q, ώστε $z_r = f_u(z_{r-1}) = q$. Και

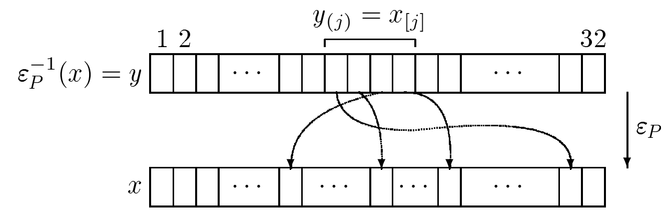
$$A = \varepsilon_E(z_{r-1}^R), \qquad B = \oplus_u A, \qquad C = S(B), \qquad D = \varepsilon_P(C)$$

θα είναι όλες οι ενδιάμεσες ακολουθίες κατά τον υπολογισμό της τιμής της συνάρτησης F στον τελευταίο γύρο. Και $p^* = z_0^*, z_1^*, \ldots, z_{r-1}^*, A^*, B^*, C^*, D^*, z_r^* = q^*$ θα είναι οι αντίστοιχες ποσότητες για το δεύτερο κρυπτοπακέτο.

Τέλος, θα χρειαστούμε μερικούς ειδικούς ορισμούς για να αναφερόμαστε εύκολα στα διάφορα κομμάτια των παραπάνω ακολουθιών.



Σχημα 2



Σχημα 3

1.1. Ορισμος. Έστω $j = 1, \ldots, 8$ και x μια δυαδική ακολουθία. Αν η x είναι 48-ψήφια, τότε ορίζουμε

$$x_{(j)} = x_{j,6}.$$

Αν η x είναι 32-ψήφια, τότε ορίζουμε

$$x_{(j)} = x_{j,4} \quad \text{και} \quad x_{\langle j\rangle} = \varepsilon_E(x)_{(j)} \quad \text{και} \quad x_{[j]} = \varepsilon_P^{-1}(x)_{(j)},$$

όπου E και P τα γνωστά διανύσματα από τον ορισμό του DES.

Για τους συμβολισμούς με την παρένθεση, η ιδέα είναι η εξής: Με $x_{(j)}$ αναφερόμαστε στο j-οστό «όγδοο» της ακολουθίας x· αν η x έχει 48 ψηφία, τότε το «όγδοό» της είναι μια εξάδα, αλλά αν έχει 32 ψηφία, το «όγδοό» της είναι μια τετράδα.

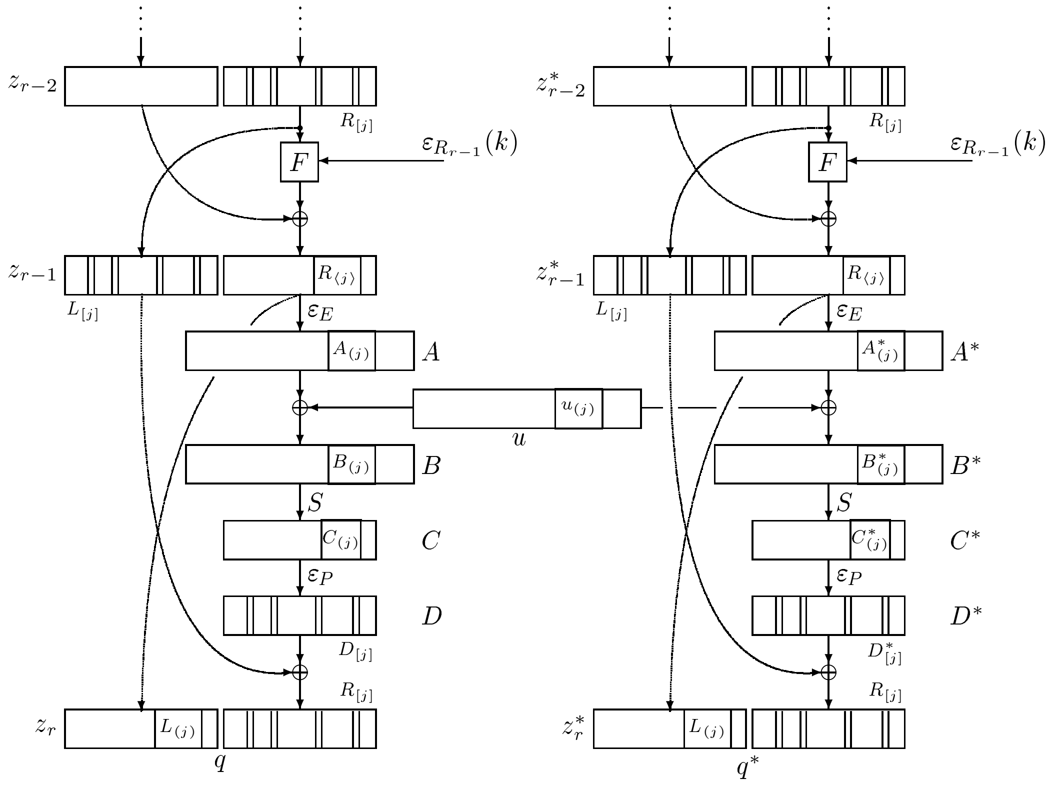
Εξάλλου, όταν η x έχει 32 ψηφία, με $x_{\langle j\rangle}$ αναφερόμαστε στην εξάδα των ψηφίων της που αποτελούν τη j-οστή εξάδα στη 48-ψήφια $E(x)$. Ισοδύναμα, πρόκειται για την εξάδα που προκύπτει από την j-οστή τετράδα της x, όταν της προθέσουμε το δεξιότερο ψηφίο της προηγούμενης τετράδας και της επιθέσουμε το αριστερότερο ψηφίο της επόμενης τετράδας (Σχήμα 2, επίσης Σχήμα 2-2).

Τέλος, για επίσης 32-ψήφια x, ο συμβολισμός $x_{[j]}$ αναφέρεται στα ψηφία της x που η μετάθεση ε_P^{-1} τα φέρνει στις θέσεις των ψηφίων της j-οστής τετράδας (Σχήμα 3).

Είναι σημαντικό να θυμόμαστε ότι, για κάθε $j = 1, \ldots, 8$, καθεμιά από τις συναρτήσεις $\cdot_{(j)}$, $\cdot_{\langle j\rangle}$ και $\cdot_{[j]}$ που μόλις ορίσαμε δεν είναι τίποτα περισσότερο από μια επιλογή (Ενότητα 1-3.1.3). Οπότε, π.χ., επιμερίζονται όλες ως προς τη διάζευξη.

2. Η τεχνική

Ας υποθέσουμε ότι, ως εχθρός, έχουμε υποκλέψει τα κρυπτοκείμενα q και q^*, και ότι ξέρουμε γι' αυτά όχι μόνο τα αντίστοιχα κείμενα, p και p^*, αλλά και τη διάζευξη $z'_{r-2} = z_{r-2} \oplus z^*_{r-2}$ —που εδώ θα τη λέμε *διαφορά*— των αντίστοιχων ενδιάμεσων αποτελεσμάτων z_{r-2} και z^*_{r-2}. Θα προσπαθήσουμε, με αυτά τα δεδομένα, να υπολογίσουμε το k. (Σχήμα 4.) Σημαντικό είναι ότι *δεν υποθέτουμε γνώση των ίδιων των z_{r-2} και z^*_{r-2}, παρά μόνο της διαφοράς τους.*



Σχημα 4

2.1. Από το k στο $u_{(j)}$. Η πρώτη εύκολη παρατήρηση είναι ότι μας αρκεί να υπολογίσουμε το υποκλειδί u του τελευταίου γύρου. Γιατί, αν μάθουμε το u, θα ξέρουμε αμέσως 48 από τα 56 ψηφία του κλειδιού (το ποια ακριβώς το βρίσκουμε εύκολα από το γνωστό διάνυσμα R_r). Οπότε θα μένει να βρούμε τα υπόλοιπα 8. Δίνοντας σε αυτά τιμές με όλους τους $2^8 = 256$ διαφορετικούς τρόπους, θα έχουμε μόνο 256 διαφορετικά ενδεχόμενα για το ποια μπορεί να είναι τελικά η σωστή τιμή του κλειδιού. Και θα μπορέσουμε εύκολα να ελέγξουμε για καθεμιά από αυτές τις πιθανές τιμές, αν πράγματι κρυπτογραφεί τα p και p^* στα q και q^* αντίστοιχα.

Προσπαθούμε λοιπόν να υπολογίσουμε το u. Για λόγους που θα φανούν στη συνέχεια, βολεύει να επικεντρώσουμε την προσπάθεια στο να υπολογίσουμε μόνο τη j-οστή εξάδα του, $u_{(j)}$, για το τυχόν $j = 1, \ldots, 8$. Αν τα καταφέρουμε, τότε με 8 παρόμοιους υπολογισμούς, έναν για κάθε j, θα έχουμε ολόκληρο το u.

2.2. Εύρεση του $u_{(j)}$. Κατ' αρχήν, εύκολα παρατηρούμε ότι

(2) $$u_{(j)} = A_{(j)} \oplus B_{(j)},$$

και ότι το $A_{(j)}$ υπολογίζεται πολύ εύκολα,

(3) $$A_{(j)} = \varepsilon_E(z^R_{r-1})_{(j)} = (z^R_{r-1})_{\langle j\rangle} = (q^L)_{\langle j\rangle}.$$

Αν μπορούσαμε να υπολογίσουμε και το $B_{(j)}$ το ίδιο εύκολα, τότε θα είχαμε τελειώσει. Αλλά αυτό δεν είναι δυνατόν.

Ένας τρόπος να προσπαθήσουμε είναι μέσω της διάζευξης που προηγείται, οπότε, με βάση και τον υπολογισμό του $A_{(j)}$,

$$B_{(j)} = A_{(j)} \oplus u_{(j)} = (q^L)_{\langle j\rangle} \oplus u_{(j)}. \tag{4}$$

Αλλά έτσι δεν κάνουμε τίποτα, αφού χρησιμοποιούμε το $u_{(j)}$.

Ο άλλος τρόπος για να προσπαθήσουμε είναι μέσω της συνάρτησης αντικατάστασης α_{S_j} που έπεται, οπότε έχουμε

$$B_{(j)} \in \alpha_{S'_j}^{-1}(C_{(j)}),$$

όπου εννοούμε ότι γενικά

$$\text{για κάθε } y \in \mathbb{B}^4, \quad \alpha_{S'_j}^{-1}(y) = \{x \in \mathbb{B}^6 \mid \alpha_{S'_j}(x) = y\}.$$

Αλλά, και πάλι, δεν μπορούμε να βρούμε την τιμή του $C_{(j)}$, γιατί

$$\begin{aligned} C_{(j)} = \varepsilon_P^{-1}(D)_{(j)} = D_{[j]} &= (z_{r-1}^L \oplus q^R)_{[j]} \\ &= (z_{r-1}^L)_{[j]} \oplus (q^R)_{[j]} = (z_{r-2}^R)_{[j]} \oplus (q^R)_{[j]}. \end{aligned} \tag{5}$$

και δεν ξέρουμε το $(z_{r-2}^R)_{[j]}$.

Το πρόβλημα διορθώνεται όταν χρησιμοποιήσουμε και τη δεύτερη σειρά από δεδομένα που έχουμε στη διάθεσή μας, δηλαδή τις ποσότητες που αντιστοιχούν στο δεύτερο κρυπτοκείμενο. Προφανώς, γι' αυτές ισχύουν τα ανάλογα των (4) και (5), δηλαδή

$$B^*_{(j)} = (q^{*L})_{\langle j\rangle} \oplus u_{(j)}, \tag{6}$$

$$C^*_{(j)} = (z^{*R}_{r-2})_{[j]} \oplus (q^{*R})_{[j]}. \tag{7}$$

Μπορούμε λοιπόν να υπολογίσουμε τη διαφορά $B'_{(j)} = B_{(j)} \oplus B^*_{(j)}$. Πράγματι, από τις (4) και (6), έχουμε ότι

$$B'_{(j)} = \big((q^L)_{\langle j\rangle} \oplus u_{(j)}\big) \oplus \big((q^{*L})_{\langle j\rangle} \oplus u_{(j)}\big) = (q^L)_{\langle j\rangle} \oplus (q^{*L})_{\langle j\rangle},$$

οπότε, από τον επιμερισμό των επιλογών ως προς τη διάζευξη,

$$B'_{(j)} = (q'^L)_{\langle j\rangle} \tag{8}$$

όπου βέβαια $q' = q \oplus q^*$.

Παρόμοια, μπορούμε να υπολογίσουμε τη διαφορά $C'_{(j)} = C_{(j)} \oplus C^*_{(j)}$, από τις (5) και (7),

$$C'_{(j)} = (z'^R_{r-2})_{[j]} \oplus (q'^R)_{[j]}, \tag{9}$$

καθώς είναι γνωστή η διαφορά z'_{r-2}.

Οπότε, τελικά, ξέρουμε για την εξάδα $B_{(j)}$ ότι: *αυτή και η κατά $B'_{(j)}$ διαφορετική της αναγκάζουν τη συνάρτηση αντικατάστασης $\alpha_{S'_j}$ να επιστρέψει τετράδες που διαφέρουν κατά $C'_{(j)}$.* Η συγκεκριμένη πληροφορία αποδεικνύεται πολύ χρήσιμη, καθώς —με κάποιες προϋποθέσεις— μπορεί να ελαττώσει σημαντικά τις πιθανές τιμές για την $B_{(j)}$.

Πιο τυπικά, αν ορίσουμε για κάθε $\alpha \in \mathbb{B}^6$ και κάθε $\beta \in \mathbb{B}^4$ το σύνολο

$$\mathrm{IN}_j(\alpha, \beta) = \{x \in \mathbb{B}^6 \mid \alpha_{S'_j}(x) \oplus \alpha_{S'_j}(x \oplus \alpha) = \beta\},$$

τότε το συμπέρασμα της προηγούμενης παραγράφου είναι ακριβώς ότι

$$B_{(j)} \in \mathrm{IN}_j(B'_{(j)}, C'_{(j)}). \tag{10}$$

Αλλά το $\mathrm{IN}_j(B'_{(j)}, C'_{(j)})$ μπορούμε να το υπολογίσουμε από τον ορισμό του, ελέγχοντας εξαντλητικά για καθεμιά από τις $2^6 = 64$ εξάδες του $\mathbb{B}^6$ αν ικανοποιεί ή όχι τη σχετική συνθήκη. Και το σημαντικό είναι ότι, με μόνη εξαίρεση την περίπτωση που $B'_{(j)} = 000000 \wedge C'_{(j)} = 0000$, το σύνολο αυτό δεν έχει περισσότερα από 16 στοιχεία.

Αυτό αποδεικνύεται με τον εξαντλητικό υπολογισμό όλων των $8 \times 64 \times 16 = 8192$ διαφορετικών συνόλων $\mathrm{IN}_j(\alpha, \beta)$, για κάθε $j = 1, \ldots, 8$, $\alpha \in \mathbb{B}^6$, $\beta \in \mathbb{B}^4$, και την πινακοποίηση των μεγεθών τους. Τα αποτέλεσματα περιέχονται στους Πίνακες 3–10 του Παραρτήματος. Είναι άμεσο να παρατηρήσει κανείς ότι το μέγεθος κάθε συνόλου είναι άρτιο και, με την εξαίρεση $1 \leq j \leq 8 \wedge \alpha = 000000 \wedge \beta = 0000$, είναι το πολύ 16.

Επομένως, αν δεν είμαστε στην εξαίρεση, η (10) ελαττώνει το μέγεθος του χώρου αναζήτησης για το $B_{(j)}$ σε το πολύ 16, και επομένως κατά

$$\frac{|\mathbb{B}^6| - |\mathrm{IN}_j(B'_{(j)}, C'_{(j)})|}{|\mathbb{B}^6|} \geq \frac{64 - 16}{64} = 0.75,$$

δηλαδή κατά τουλάχιστον 75%.

Τώρα μπορούμε να επιστρέψουμε στην εξάδα $u_{(j)}$, για την οποία ξεκίνησε όλη η κουβέντα. Από τις (2), (3), (8), (9) και (10) προκύπτει ότι τελικά[2]

$$(*) \qquad u_{(j)} \quad \in \quad (q^L)_{\langle j \rangle} \boxplus \mathrm{IN}_j\Big(\, (q'^L)_{\langle j \rangle},\ (z'^R_{r-2})_{[j]} \oplus (q'^R)_{[j]} \,\Big),$$

κι έτσι το μέγεθος του χώρου αναζήτησης για το $u_{(j)}$ είναι επίσης μειωμένο σε το πολύ 16. Είναι σημαντικό ότι ο νέος χώρος αναζήτησης εξαρτάται μόνο από υπακολουθίες των κρυπτοκειμένων q, q^* και της διαφοράς z'_{r-2} των εισόδων του προτελευταίου γύρου του Feistel δικτύου. Για να φανεί αυτό, ορίζουμε ένα σύμβολο για το χώρο

$$(11) \qquad \delta_j(q, q^*, z'_{r-2}) = (q^L)_{\langle j \rangle} \boxplus \mathrm{IN}_j\Big(\, (q'^L)_{\langle j \rangle},\ (z'^R_{r-2})_{[j]} \oplus (q'^R)_{[j]} \,\Big).$$

Επίσης, η μείωση ισχύει μόνο όταν δεν είμαστε στην εξαιρετική περίπτωση που αναφέραμε πιο πάνω, δηλαδή μόνο αν

$$(q'^L)_{\langle j \rangle} \neq 000000 \quad \vee \quad (z'^R_{r-2})_{[j]} \neq (q'^R)_{[j]}.$$

Η ελάττωση του χώρου αναζήτησης μπορεί να γίνει ακόμη μεγαλύτερη, αν έχουμε στη διάθεσή μας περισσότερα από ένα ζευγάρια κρυπτοκειμένων σαν τα q και q^*. Γιατί τότε μπορούμε να υπολογίσουμε την τομή όλων των συνόλων $\delta_j(q, q^*, z'_{r-2})$ που προκύπτουν, κι αυτή

- θα περιέχει το $u_{(j)}$, προφανώς, και
- θα είναι μικρότερη από καθένα από τα $\delta_j(q, q^*, z'_{r-2})$.

Στην καλύτερη περίπτωση, η τομή θα είναι μονοσύνολο και το $u_{(j)}$ θα έχει προσδιοριστεί μονοσήμαντα. Και είναι τόσο πιο πιθανό να συμβεί αυτό, όσο πιο πολλά είναι τα ζευγάρια κρυπτοκειμένων που έχουμε στη διάθεσή μας.

Επομένως, ο αλγόριθμος για τον υπολογισμό της $u_{(j)}$ είναι ο εξής:

Αλγόριθμος 1

---

[2] Με $\boxplus$ συμβολίζουμε βεβαίως την πράξη $\boxplus : \mathbb{B}^6 \times \mathbb{P}(\mathbb{B}^6) \to \mathbb{P}(\mathbb{B}^6)$, που για κάθε εξάδα x και κάθε σύνολο εξάδων Y επιστρέφει το σύνολο των εξάδων $x \boxplus Y = \{x \oplus y \mid y \in Y\}$. Είναι μια εύκολη (και σημαντική) παρατήρηση ότι τα $x \boxplus Y$ και Y είναι ισοπληθικά.

Είσοδος: N διαφορετικά ζευγάρια κρυπτοκειμένων (q_i, q_i^*),
και οι αντίστοιχες διαφορές $(z'_{r-2})_i$ $(1 \le i \le N)$.
Έξοδος: Ένα σύνολο $U \subseteq \mathbb{B}^6$ που περιέχει τη σωστή τιμή της $u_{(j)}$.
Μέθοδος: 1. Θεώρησε $2^6 = 64$ μετρητές, c_x $(x \in \mathbb{B}^6)$, έναν για κάθε πιθανή τιμή της $u_{(j)}$, με αρχική τιμή μηδέν.
2. Για κάθε $i = 1, \ldots, N$:
2α. Υπολόγισε το σύνολο $\delta_j\big(q_i, q_i^*, (z'_{r-2})_i\big)$.
2β. Αύξησε κατά 1 κάθε μετρητή που αντιστοιχεί σε εξάδα που περιέχεται στο σύνολο, δηλ.
$$x \in \delta_j\big(q_i, q_i^*, (z'_{r-2})_i\big) \Longrightarrow c_x \longleftarrow c_x + 1.$$
3. Επέστρεψε το σύνολο $U = \{x \in \mathbb{B}^6 \mid c_x = N\}$ των εξάδων που εμφανίστηκαν σε όλα τα σύνολα.

Το σύνολο U του βήματος 3 είναι η ζητούμενη τομή. Βεβαίως, είναι εύκολο να σκεφτεί κανείς λιγότερο πολύπλοκους τρόπους για να υπολογίσει αυτήν την τομή· όμως αυτός που διαλέξαμε είναι ο πιο χρήσιμος για τη συνέχεια.

Επίσης, είναι σημαντικό ότι ο αλγόριθμος δουλεύει για κάθε $j = 1, \ldots, 8$, και μάλιστα με τα ίδια κάθε φορά δεδομένα. Είναι άμεση η τροποποίησή του που με είσοδο τα κοινά αυτά δεδομένα θα δίνει στην έξοδο 8 σύνολα εξάδων, ένα για κάθεμια από τις $u_{(1)}, \ldots, u_{(8)}$.

2.3. Από το $u_{(j)}$ στο k. Από την προηγούμενη ενότητα φαίνεται ότι, με τα σωστά δεδομένα, μπορούμε να περιορίσουμε τις πιθανές τιμές του $u_{(j)}$ από 64 που ήταν αρχικά σε το πολύ 16 και μετά ίσως και σε ακόμη λιγότερες.

Αυτό συνεπάγεται ότι τελικά θα υπάρχουν το πολύ $16^8 = 2^{32}$ διαφορετικές τιμές για ολόκληρο το υποκλειδί u. Αν λάβουμε υπόψη μας και τα 8 ψηφία του κλειδιού k που δε συμμετέχουν στο u, μένουμε τελικά με το πολύ 2^{40} διαφορετικές τιμές για το k, από 2^{56} που ήταν αρχικά. Επομένως, ο χώρος αναζήτησης για ολόκληρο το κλειδί έχει μειωθεί κατά τουλάχιστον $2^{16} = 65536$ φορές.

Στην πράξη περιμένουμε το πραγματικό πλήθος των πιθανών τιμών που θα προκύψουν να είναι πολύ μικρότερο από το απαισιόδοξο άνω φράγμα του 2^{40}. Αυτό θα προκύψει μόνο στην πολύ σπάνια περίπτωση που τα επιλεγμενα κρυπτοκείμενα είναι τέτοια ώστε για κάθε $B_{(j)}$ να υπάρχουν ακριβώς 16 πιθανές τιμές.

2.4. Το πρόβλημα. Η όλη συζήτηση βασίζεται βέβαια στην υπόθεση ότι έχουμε πράγματι τα δεδομένα που ζητήσαμε: ένα ζευγάρι (ή περισσότερα) κρυπτοκειμένων q και q^*, για τα οποία

(i) να γνωρίζουμε τα αντίστοιχα κείμενα p και p^*, και
(ii) να γνωρίζουμε τη διαφορά z'_{r-2} των εισόδων του προτελευταίου γύρου.

Μέχρι και το (i), δεν έχουμε τίποτε περισσότερο από τις υποθέσεις μιας επίθεσης με γνωστά κείμενα. Αλλά, δυστυχώς, το (ii) δεν μπορεί να εξασφαλιστεί με καμιά από τις υποθέσεις της Ενότητας 3-1.

Βεβαίως, στην ειδική περίπτωση που η συνάρτηση κρυπτογράφησης έχει μόνο 2 Feistel γύρους $(r = 2)$, τότε οι είσοδοι στον προτελευταίο γύρο είναι ακριβώς τα κείμενα, άρα
$$z'_{r-2} = z'_0 = z_0 \oplus z_0^* = p \oplus p^*,$$
και η υπόθεση των γνωστών κειμένων μας καλύπτει και για το (ii). Αλλά η πραγματικότητα είναι ότι $r = 16$.

Ακόμα και στην περίπτωση που $r = 3$, μπορούμε να κάνουμε κάτι: Διαλέγοντας τα p και p^* έτσι που να έχουν το ίδιο δεξί μισό, $p^R = p^{*R}$, εξασφαλίζουμε ότι

$$F_{\varepsilon_{R_{r-2}}(k)}(p^R) = F_{\varepsilon_{R_{r-2}}(k)}(p^{*R}),$$

και επομένως μπορούμε να υπολογίσουμε

$$\begin{aligned} z'^R_{r-2} &= z^R_{r-2} \oplus z^{*R}_{r-2} \\ &= \big(z^L_{r-3} \oplus F_{\varepsilon_{R_{r-2}}(k)}(z^R_{r-3})\big) \oplus \big(z^{*L}_{r-3} \oplus F_{\varepsilon_{R_{r-2}}(k)}(z^{*R}_{r-3})\big) \\ &= \big(p^L \oplus F_{\varepsilon_{R_{r-2}}(k)}(p^R)\big) \oplus \big(p^{*L} \oplus F_{\varepsilon_{R_{r-2}}(k)}(p^{*R})\big) \\ &= p^L \oplus p^{*L} \\ &= p'^L. \end{aligned}$$

Επίσης, τετριμμένα ξέρουμε ότι

$$z'^L_{r-2} = z^L_{r-2} \oplus z^{*L}_{r-2} = z^R_{r-3} \oplus z^{*R}_{r-3} = p^R \oplus p^{*R} = \underbrace{00\cdots00}_{32}.$$

Οπότε τελικά ξέρουμε το $z'_{r-2} = 00\cdots00 \,\|\, p'^L$, και η υπόθεση των γνωστών κειμένων μας καλύπτει για το (ii), και πάλι. Αλλά η πραγματικότητα είναι ότι $r = 16$.

Η ιδέα είναι ότι όσο περισσότεροι είναι οι Feistel γύροι στη συνάρτηση κρυπτογράφησης, τόσο πιο δύσκολο είναι να υπολογίσουμε τη διαφορά z'_{r-2} από τα κείμενα p και p^*. Και ήδη για $r = 4$ αυτό γίνεται αδύνατο, όπως μπορεί κανείς να επιβεβαιώσει δοκιμάζοντας. Η αιτία είναι βεβαίως το απρόβλεπτο του τρόπου με τον οποίον τα άγνωστα σε μας υποκλειδιά των γύρων $1, 2, \ldots, r-3$ επηρεάζουν την z'_{r-2}.

2.5. Η λύση. Αφού λοιπόν δεν μπορούμε να *υπολογίσουμε* τη διαφορά z'_{r-2}, το επόμενο καλύτερο που μπορούμε να κάνουμε είναι να προσπαθήσουμε να την *προβλέψουμε*. Η ιδέα προκύπτει από τη δυνατότητα που (θα φανεί παρακάτω ότι) έχουμε να διαλέγουμε ένα ζευγάρι κειμένων p και p^* στην είσοδο του πρώτου Feistel γύρου έτσι που να ξέρουμε την πιθανότητα, έστω π, με την οποία η διαφορά z'_{r-2} θα πάρει κάποια συγκεκριμένη τιμή, έστω z.

Τότε δοκιμάζοντας N διαφορετικά ζευγάρια, $(p_1, p_1^*), (p_2, p_2^*), \ldots, (p_N, p_N^*)$, μπορούμε να περιμένουμε ότι οι $N\pi$ από τις αντίστοιχες διαφορές $(z'_{r-2})_1, (z'_{r-2})_2, \ldots,$ $(z'_{r-2})_N$ θα έχουν πράγματι την τιμή z, ενώ οι υπόλοιπες θα έχουν άλλες, τυχαίες τιμές. Τότε σε $N\pi$ από τις περιπτώσεις θα ισχύει το συμπέρασμα $(*)$, ενώ στις υπόλοιπες $N(1-\pi)$ δεν θα ισχύει· δηλαδή $N\pi$ από τα σύνολα

$$\delta_j\big(q_i, q_i^*, (z'_{r-2})_i\big) \qquad (1 \le i \le N)$$

πράγματι θα περιέχουν τη σωστή τιμή για το $u_{(j)}$ και θα τα λέμε «έγκυρα» σύνολα, ενώ τα υπόλοιπα $N(1-\pi)$ θα περιέχουν τυχαίες τιμές και θα τα λέμε «άκυρα» σύνολα.

Ο Αλγόριθμος 1 θα μπορούσε να δουλέψει άμεσα, αν ξέραμε ποια ακριβώς από τα σύνολα είναι έγκυρα και ποια είναι άκυρα. Τότε θα ξεχωρίζαμε τα έγκυρα και θα εφαρμόζαμε τον αλγόριθμο μόνο πάνω σε αυτά. Όμως δεν μπορούμε να κάνουμε αυτή τη διάκριση.

Παρόλ' αυτά, ο Αλγόριθμος 1 συνεχίζει να είναι χρήσιμος. Αν τον εφαρμόσουμε πάνω και στα N ζευγάρια κρυπτοκειμένων, τότε κάθε μετρητής c_x ($x \in \mathbb{B}^6$) θα πάρει μια τελική τιμή που θα είναι το άθροισμα δύο συνιστωσών, c'_x και c''_x: η πρώτη από τη συμμετοχή της x στα έγκυρα σύνολα και η δεύτερη από τη συμμετοχή της x στα άκυρα σύνολα. Υποθέτοντας ότι τα άκυρα σύνολα είναι αρκετά ομοιόμορφα τυχαία, μπορούμε να περιμένουμε ότι οι δεύτερες συνιστώσες των μετρητών δεν θα διαφέρουν πολύ μεταξύ τους, δηλαδή

$$c''_{x_1} \approx c''_{x_2},$$

για κάθε δύο $x_1, x_2 \in \mathbb{B}^6$. Παρόμοια, υποθέτοντας ότι οι λάθος εξάδες που περιέχονται στα έγκυρα σύνολα είναι επίσης αρκετά ομοιόμορφα τυχαίες, μπορούμε να περιμένουμε ότι και οι πρώτες συνιστώσες των μετρητών που αντιστοιχούν σε αυτές τις εξάδες δεν θα διαφέρουν πολύ μεταξύ τους, δηλαδή

$$c'_{x_1} \approx c'_{x_2},$$

για κάθε $x_1, x_2 \in \mathbb{B}^6 \setminus \{x_0\}$, με x_0 τη σωστή τιμή για τη $u_{(j)}$. Όμως η πρώτη συνιστώσα του μετρητή c_{x_0} της σωστής τιμής x_0 περιμένουμε να είναι κοντά στο $N\pi$.

Πιο αναλυτικά, αν υποθέσουμε ότι καθένα από τα έγκυρα σύνολα έχει μέγεθος λ, τότε μια εκτίμηση για την πρώτη συνιστώσα κάποιας λάθος τιμής $x \in \mathbb{B}^6 \setminus \{x_0\}$, είναι η

$$c'_x \approx \frac{N\pi\lambda - N\pi}{63}$$

κι έτσι μια εκτίμηση για τη διαφορά των μετρητών c_{x_0} και c_x είναι η

$$c_{x_0} - c_x = (c'_{x_0} - c'_x) + (c''_{x_0} - c''_x) \approx \big(N\pi - \frac{N\pi\lambda - N\pi}{63}\big) + 0 = N\pi\frac{62-\lambda}{63}.$$

Αν λοιπόν το γινόμενο $N\pi$ είναι αρκετά μεγάλο, τότε μπορούμε να περιμένουμε ότι ο μετρητής c_{x_0} θα ξεχωρίσει από τους υπόλοιπους, αναδεικνύοντας έτσι τη σωστή τιμή για τη $u_{(j)}$.

Στην πράξη, οι τιμές που ξεχωρίζουν με αυτόν τον τρόπο είναι περισσότερες από μια, αλλά και πάλι το πλήθος τους παραμένει πολύ μικρότερο από το πλήθος 64 όλων των δυνατών τιμών.

Τελικά, ο νέος αλγόριθμος έχει ως εξής:

Αλγόριθμος 2

Έξοδος: Ένα σύνολο $U \subseteq \mathbb{B}^6$ που (περιμένουμε να) περιέχει τη σωστή τιμή της $u_{(j)}$.

Μέθοδος:
0. Διάλεξε N ζευγάρια κειμένων (p_i, p_i^*) $(1 \le i \le N)$, έτσι που κάθε φορά να είναι π η πιθανότητα ότι η αντίστοιχη διαφορά $(z'_{r-2})_i$ είναι z. Ας είναι (q_i, q_i^*) τα αντίστοιχα κρυπτοκείμενα.
1. Θεώρησε $2^6 = 64$ μετρητές, c_x $(x \in \mathbb{B}^6)$, έναν για κάθε πιθανή τιμή της $u_{(j)}$, με αρχική τιμή μηδέν.
2. Για κάθε $i = 1, \ldots, N$:
   - 2α. Υπολόγισε το σύνολο $\delta_j(q_i, q_i^*, z)$.
   - 2β. Αύξησε κατά 1 κάθε μετρητή που αντιστοιχεί σε εξάδα που περιέχεται στο σύνολο, δηλ.
     $$x \in \delta_j(q_i, q_i^*, z) \Longrightarrow c_x \longleftarrow c_x + 1.$$
3. Επέστρεψε το σύνολο U των εξάδων που αντιστοιχούν στους k πιο μεγάλους μετρητές, για κάποιο $k \ge 1$.

Βεβαίως, δεν έχουμε ακόμη πει πώς πρέπει να γίνεται η επιλογή των N κειμένων στο βήμα 0, ώστε να εξασφαλίζεται η εμφάνιση της διαφοράς z με τη συγκεκριμένη γνωστή πιθανότητα π.

Μια πρώτη ιδέα είναι να διαλέγουμε κάθε ζευγάρι (p, p^*) ομοιόμορφα και τυχαία μέσα από το σύνολο όλων των ζευγών κειμένων. Τότε θα είναι ομοιόμορφα τυχαίο και το κάθε ζευγάρι (z_i, z_i^*) ενδιάμεσων αποτελεσμάτων στο Feistel δίκτυο, ακριβώς επειδή κάθε Feistel μετάθεση είναι μια μετάθεση του $\mathbb{B}^{64}$. Επομένως, θα είναι ομοιόμορφα τυχαίο και το (z_{r-2}, z_{r-2}^*). Το οποίο σημαίνει ότι η διαφορά z'_{r-2} θα είναι επίσης ομοιόμορφα τυχαία μέσα στο σύνολο $\mathbb{B}^{64}$ όλων των διαφορών πακέτων. Άρα, για το τυχόν $z \in \mathbb{B}^{64}$, η πιθανότητα ότι $z'_{r-2} = z$ θα είναι

$$\pi = \frac{1}{2^{64}}.$$

Οπότε, για να γίνει το γινόμενο $N\pi$ αρκετά μεγάλο, θα πρέπει το πλήθος N να γίνει σημαντικά μεγαλύτερο από 2^{64}. Αλλά αυτό αμέσως κάνει το κόστος της επίθεσης συγκρίσιμο με αυτό των τετριμμένων επιθέσεων (βλέπε την Ενότητα 3-4 και τον Ορισμό 3-5.2), που σημαίνει ότι η επίθεση καθόλου δεν προσβάλλει την ασφάλεια του κρυπτοσυστήματος.

Επομένως, ο χώρος επιλογής των ζευγών κειμένων δεν μπορεί να είναι όλο το $\mathbb{B}^{64} \times \mathbb{B}^{64}$. Όπως θα φανεί τελικά, μια καλή επιλογή αυτού του χώρου είναι το σύνολο των ζευγαριών πακέτων που έχουν κάποια συγκεκριμένη διαφορά, δηλαδή το

$$\{(p, p^*) \in \mathbb{B}^{64} \times \mathbb{B}^{64} \mid p \oplus p^* = p'\},$$

για κάποιο κατάλληλα επιλεγμένο $p' \in \mathbb{B}^{64}$. Τότε η πιθανότητα π γίνεται αρκετά μεγάλη, ώστε το πλήθος N να μπορεί να διατηρηθεί αρκετά μικρό, ώστε η επίθεση πράγματι να προσβάλλει το κρυπτοσύστημα.

3. Διαφορικά αιτιοκρατικοί τελεστές

Τελικά βρισκόμαστε στην κατάσταση που πρέπει να μελετήσουμε τον τρόπο με τον οποίον οι τελεστές που συνιστούν ένα κρυπτοσύστημα μεταδίδουν τις διαφορές από τις εισόδους προς τις εξόδους τους. Το πρώτο βήμα προς αυτή την κατεύθυνση είναι ο επόμενος ορισμός.

3.1. Ορισμος. Έστω $T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \to \mathbb{B}^{n}$ τυχών τελεστής και $\overline{x} = (x_1, \ldots, x_\lambda), \overline{x}^* = (x_1^*, \ldots, x_\lambda^*) \in \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda}$. Λέμε *εξοδοδιαφορά των* $\overline{x}$, $\overline{x}^*$ *ως προς τον* T τη διαφορά

$$T(\overline{x}) \oplus T(\overline{x}^*)$$

των εξόδων του T για εισόδους $\overline{x}$ και $\overline{x}^*$.

Τώρα κατηγοριοποιούμε τους τελεστές ως προς τον τρόπο με τον οποίον αποφασίζουν τις εξοδοδιαφορές των ζευγαριών εισόδων τους.

3.2. Ορισμος. Λέμε ότι ο τελεστής $T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \to \mathbb{B}^{n}$ είναι *διαφορικά αιτιοκρατικός* αν υπάρχει συνάρτηση

$$\sigma_T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \to \mathbb{B}^{n}$$

τέτοια που για κάθε $\overline{x} = (x_1, \ldots, x_\lambda), \overline{x}^* = (x_1^*, \ldots, x_\lambda^*) \in \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda}$ να είναι

$$T(\overline{x}) \oplus T(\overline{x}^*) = \sigma_T(\overline{x}'),$$

όπου $\overline{x}' = \overline{x} \oplus \overline{x}^* = (x_1 \oplus x_1^*, \ldots, x_\lambda \oplus x_\lambda^*)$. Ονομάζουμε την σ_T *διαφορικό αντίστοιχο του* T.

Δηλαδή ο T είναι δ. αιτιοκρατικός αν η εξοδοδιαφορά των τυχόντων $\overline{x}$, $\overline{x}^*$ ως προς τον T εξαρτάται μόνο από τη διαφορά τους $\overline{x} \oplus \overline{x}^*$ και όχι από τα ίδια τα $\overline{x}$ και $\overline{x}^*$. Υπάρχουν πολλά παραδείγματα τέτοιων τελεστών.

3.3. Πρόταση. *Έστω $l, l_1, l_2 \geq 1$.*

(i) *Η διαφορά (διάζευξη) $\oplus : \mathbb{B}^l \times \mathbb{B}^l \to \mathbb{B}^l$ είναι δ. αιτιοκρατική, με δ. αντίστοιχο τον εαυτό της.*

(ii) *Για κάθε $u \in \mathbb{B}^l$, η διαφορά με τη u, $\oplus_u : \mathbb{B}^l \to \mathbb{B}^l$, είναι δ. αιτιοκρατική, με δ. αντίστοιχο την ταυτοτική συνάρτηση $\mathrm{i} : \mathbb{B}^l \to \mathbb{B}^l$.*

(iii) *Οποιαδήποτε επιλογή $\varepsilon : \mathbb{B}^{l_1} \to \mathbb{B}^{l_2}$ είναι δ. αιτιοκρατική, με δ. αντίστοιχο τον εαυτό της.*

(iv) *Η παράθεση $\| : \mathbb{B}^{l_1} \times \mathbb{B}^{l_2} \to \mathbb{B}^{l_1+l_2}$ είναι δ. αιτιοκρατική, με δ. αντίστοιχο τον εαυτό της.*

Απόδειξη. Εύκολα, για κατάλληλα κάθε φορά ορίσματα,

$$\begin{aligned}
\oplus(\overline{x}) \;\oplus\; \oplus(\overline{x}^*) &= \oplus(x_1, x_2) \;\oplus\; \oplus(x_1^*, x_2^*) = (x_1 \oplus x_2) \oplus (x_1^* \oplus x_2^*) \\
&= (x_1 \oplus x_1^*) \oplus (x_2 \oplus x_2^*) = x_1' \oplus x_2' = \oplus(\overline{x}'), \\
\oplus_u(x) \;\oplus\; \oplus_u(x^*) &= (x \oplus u) \oplus (x^* \oplus u) = x \oplus x^* = x', \\
\varepsilon(x) \oplus \varepsilon(x^*) &= \varepsilon(x \oplus x^*) = \varepsilon(x'), \\
\|(\overline{x}) \;\oplus\; \|(\overline{x}^*) &= \|(x_1, x_2) \;\oplus\; \|(x_1^*, x_2^*) = (x_1 \,\|\, x_2) \oplus (x_1^* \,\|\, x_2^*) \\
&= (x_1 \oplus x_1^*) \,\|\, (x_2 \oplus x_2^*) = x_1' \,\|\, x_2' = \|(\overline{x}').
\end{aligned}$$

Άρα $\sigma_\oplus = \oplus$, $\sigma_{\oplus_u} = \mathrm{i}$, $\sigma_\varepsilon = \varepsilon$ και $\sigma_\| = \|$. ⊣

3.4. Πόρισμα. *Για τα κατάλληλα j, m (βλέπε στην Ενότητα 1-3.1.4 και τον Ορισμό 1.1), καθεμιά από τις συναρτήσεις $\cdot_{j,m}$, $\cdot^L$, $\cdot^R$, $\circlearrowleft$, $\cdot_{(j)}$, $\cdot_{\langle j\rangle}$ και $\cdot_{[j]}$ είναι δ. αιτιοκρατική με δ. αντίστοιχο τον εαυτό της.*

Απόδειξη. Όλες αυτές οι συναρτήσεις είναι επιλογές. ⊣

Τώρα ονοματίζουμε ένα πολύ συχνό φαινόμενο, που εμφανίστηκε ήδη.

3.5. Ορισμός. Λέμε ότι ο διαφορικά αιτιοκρατικός τελεστής T είναι *διαφορικά αμετάβλητος*, αν ταυτίζεται με το διαφορικό του αντίστοιχο, αν δηλαδή

$$\sigma_T = T.$$

3.6. Παρατήρηση. Επομένως, όλοι οι παραπάνω τελεστές (Προταση 3.3 και Πόρισμα 3.4) είναι διαφορικά αμετάβλητοι, με μόνη εξαίρεση τον $\oplus_u$.

Αλλά δεν είναι όλοι οι τελεστές διαφορικά αιτιοκρατικοί, και δύο παραδείγματα είναι τα επόμενα.

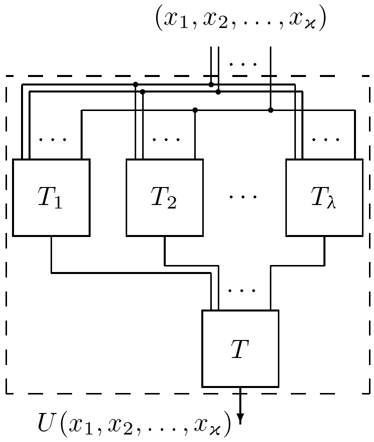
3.7. Πρόταση. *Η συνάρτηση αντικατάστασης α_{S_1} που ορίζεται από τον πρώτο πίνακα αντικατάστασης S_1 του DES είναι διαφορικά μη αιτιοκρατική.*

Απόδειξη. Είναι $\alpha_{S_1} : \mathbb{B}^6 \to \mathbb{B}^4$ και αρκεί να βρούμε δυο ζευγάρια εισόδων, έστω (x_1, x_1^*) και (x_2, x_2^*), που να έχουν την ίδια διαφορά αλλά άλλη εξοδοδιαφορά ως προς τον α_{S_1},

$$x_1 \oplus x_1^* = x_2 \oplus x_2^* \qquad \text{και} \qquad \alpha_{S_1}(x_1) \oplus \alpha_{S_1}(x_1^*) \neq \alpha_{S_1}(x_2) \oplus \alpha_{S_1}(x_2^*).$$

Τέτοια είναι, π.χ., τα $(x_1, x_1^*) = (000000, 001000)$ και $(x_2, x_2^*) = (000001, 001001)$, με κοινή διαφορά 001000, αλλά εξοδοδιαφορές 1101 και 1110 αντίστοιχα. ⊣

3.8. Πόρισμα. *Ο τελεστής S του DES είναι διαφορικά μη αιτιοκρατικός.*



Σχημα 5

Αποδειξη. Όπως και στην προηγούμενη απόδειξη, χρησιμοποιώντας τα

$$(x_1, x_1^*) = (000000 \,\|\, y, 001000 \,\|\, y) \quad \text{και} \quad (x_2, x_2^*) = (000001 \,\|\, y, 001001 \,\|\, y),$$

για οποιοδήποτε $y \in \mathbb{B}^{42}$. ⊣

Βασική ιδιότητα της διαφορικής αιτιοκρατικότητας είναι ότι διατηρείται κατά τη σύνθεση.

3.9. Προταση. *Κάθε σύνθεση διαφορικά αιτιοκρατικών τελεστών είναι ένας επίσης διαφορικά αιτιοκρατικός τελεστής, με διαφορικό αντίστοιχο τη σύνθεση των διαφορικών αντιστοίχων.*

Αποδειξη. Αρκεί να δείξουμε ότι αν οι τελεστές

$$T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \to \mathbb{B}^{n}, \text{ και}$$
$$T_i : \mathbb{B}^{m_1} \times \cdots \times \mathbb{B}^{m_\varkappa} \to \mathbb{B}^{n_i} \qquad (1 \le i \le \lambda)$$

είναι δ. αιτιοκρατικοί, τότε το ίδιο ισχύει και για τη σύνθεσή τους (Σχήμα 5),

$$U : \mathbb{B}^{m_1} \times \cdots \times \mathbb{B}^{m_\varkappa} \to \mathbb{B}^{n}, \text{ με}$$
$$U(x_1, \ldots, x_\varkappa) = T\big(T_1(x_1, \ldots, x_\varkappa), \ldots, T_\lambda(x_1, \ldots, x_\varkappa)\big).$$

Πράγματι, για τυχόντα $\overline{x} = (x_1, \ldots, x_\varkappa)$ και $\overline{x}^* = (x_1^*, \ldots, x_\varkappa^*)$ είναι

$$\begin{aligned} U(\overline{x}) \oplus U(\overline{x}^*) &= T\big(T_1(\overline{x}), \ldots, T_\lambda(\overline{x})\big) \oplus T\big(T_1(\overline{x}^*), \ldots, T_\lambda(\overline{x}^*)\big) \\ &= \sigma_T\big(T_1(\overline{x}) \oplus T_1(\overline{x}^*), \ldots, T_\lambda(\overline{x}) \oplus T_\lambda(\overline{x}^*)\big) \\ &= \sigma_T\big(\sigma_{T_1}(\overline{x} \oplus \overline{x}^*), \ldots, \sigma_{T_\lambda}(\overline{x} \oplus \overline{x}^*)\big) \\ &= \big(\sigma_T \circ (\sigma_{T_1}, \ldots, \sigma_{T_\lambda})\big)(\overline{x} \oplus \overline{x}^*). \end{aligned}$$

Ώστε ο U είναι κι αυτός δ. αιτιοκρατικός, και το διαφορικό του αντίστοιχο είναι η συνάρτηση $\sigma_U = \sigma_T \circ (\sigma_{T_1}, \ldots, \sigma_{T_\lambda})$. ⊣

3.10. Παρατηρηση. Το αντίστροφο της πρότασης δεν ισχύει: η σύνθεση κάποιων τελεστών μπορεί να είναι δ. αιτιοκρατική και κάποιος από αυτούς να μην είναι. Για ένα προφανές αντιπαράδειγμα, αν ο τελεστής T της παραπάνω απόδειξης είναι σταθερός (επιστρέφει την ίδια τιμή, για κάθε είσοδο), τότε ο U είναι δ. αιτιοκρατικός, ανεξάρτητα από το τι είναι καθένας από τους T_i $(1 \le i \le \lambda)$.

Από την Πρόταση 3.9 μπορούμε να βγάλουμε τα επόμενα άμεσα συμπεράσματα.

3.11. Πόρισμα. *Η σύνθεση διαφορικά αμετάβλητων τελεστών είναι διαφορικά αμετάβλητος τελεστής.*

3.12. Πόρισμα. *Κάθε Feistel μετάθεση και κάθε Feistel πολυμετάθεση πάνω από διαφορικά αιτιοκρατική συνάρτηση είναι ένας διαφορικά αιτιοκρατικός τελεστής.*

Απόδειξη. Αν η συνάρτηση F πάνω από την οποία ορίζονται η Feistel μετάθεση και η Feistel πολυμετάθεση είναι δ. αιτιοκρατική, τότε (εύκολα) το ίδιο ισχύει και για την παραμετρική εκδοχή της, F_u, για κάθε νόμιμο u. Οπότε, το πρώτο σκέλος έπεται από τον ορισμό (1-3.4) της Feistel μετάθεσης ως σύνθεσης των $\|$, $\oplus$, $\cdot^L$, $\cdot^R$ και F_u. Και το δεύτερο προκύπτει από τον ορισμό (1-3.5) της Feistel πολυμετάθεσης ως σύνθεσης Feistel μεταθέσεων και της $\circlearrowleft$. ⊣

3.13. Πόρισμα. *Αν ο τελεστής S του DES ήταν διαφορικά αιτιοκρατικός, τότε το DES θα προσβάλλονταν άμεσα από την κρυπταναλυτική επίθεση του Αλγορίθμου 2.*

Απόδειξη. Αν ο S ήταν δ. αιτιοκρατικός, τότε το ίδιο θα ίσχυε και για τη συνάρτηση F του DES, που ορίζεται ως σύνθεση δύο επιλογών, μιας λεύκανσης και του S. Οπότε, κάθε Feistel μετάθεση στην e_k θα ήταν δ. αιτιοκρατική. Και επομένως το ίδιο θα ίσχυε και για τη σύνθεση των πρώτων $r-2$ από αυτές. Άρα, δεδομένης της διαφοράς $p' = p \oplus p^*$ των κειμένων στην είσοδο της συνάρτησης κρυπτογράφησης, θα ήταν δεδομένη η διαφορά $z'_{r-2} = z_{r-2} \oplus z^*_{r-2}$ των εισόδων του προτελευταίου γύρου, δηλαδή προβλέψιμη με πιθανότητα $\pi = 1$. Οπότε το γινόμενο $N\pi$ θα ήταν τόσο μεγάλο όσο και το N. ⊣

Το συμπέρασμα είναι ότι η όποια αντοχή του DES στον Αλγόριθμο 2 οφείλεται ακριβώς στον τελεστή S. Στην επόμενη ενότητα συζητάμε ακόμη πιο αναλυτικά την προσφορά του S.

4. Διαφορική συμπεριφορά τελεστή

Εξ ορισμού, σε έναν τελεστή T που δεν είναι διαφορικά αιτιοκρατικός δεν μπορούμε να υπολογίσουμε την εξοδοδιαφορά δύο εισόδων του, $\overline{x}$ και $\overline{x}^*$, μόνο από τη διαφορά τους $\overline{x}' = \overline{x} \oplus \overline{x}^*$· πρέπει να ξέρουμε και τις ίδιες τις εισόδους. Σ' αυτή την περίπτωση, το επόμενο καλύτερο που μπορούμε να κάνουμε προς το να αποκτήσουμε κάποια περισσότερη πληροφορία για την εξοδοδιαφορά, είναι να προσπαθήσουμε να την προβλέψουμε με κάποια πιθανότητα.

Για κάθε δυνατή διαφορά $\overline{\alpha}$ βρίσκουμε όλα τα ζευγάρια εισόδων $(\overline{x}, \overline{x}^*)$ που διαφέρουν κατά τόσο και για καθένα από αυτά υπολογίζουμε την αντίστοιχη εξοδοδιαφορά

$$\beta = T(\overline{x}) \oplus T(\overline{x}^*).$$

Στη συνέχεια φτιάχνουμε έναν πίνακα N_T με τόσες γραμμές όσες διαφορές και τόσες στήλες όσες εξοδοδιαφορές, και με το τυχόν στοιχείο του $\mathrm{N}_T(\overline{\alpha}, \beta)$ να είναι το πλήθος των ζευγαριών εισόδων που έχουν διαφορά $\overline{\alpha}$ και εξοδοδιαφορά β. Τότε, κάθε φορά που γνωρίζουμε τη διαφορά, έστω $\overline{\alpha}$, δύο άγνωστων εισόδων, μπορούμε να ανατρέχουμε στη γραμμή της $\overline{\alpha}$ στον παραπάνω πίνακα και από τις τιμές της να παίρνουμε μια ιδέα για το ποιες εξοδοδιαφορές είναι περισσότερο «πιθανό» να συμβούν.

Τα παραπάνω γίνονται πιο συγκεκριμένα με τους ορισμούς που ακολουθούν.

4.1. Ορισμος. Ας είναι $T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \to \mathbb{B}^n$ τυχών τελεστής. Για κάθε διαφορά $\overline{\alpha}$ στοιχείων του $\mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda}$ και κάθε διαφορά β στοιχείων του $\mathbb{B}^n$, ορίζουμε το σύνολο

$$\Delta_T(\overline{\alpha}, \beta) = \{(\overline{x}, \overline{x}^*) \mid \overline{x} \oplus \overline{x}^* = \overline{\alpha} \ \wedge \ T(\overline{x}) \oplus T(\overline{x}^*) = \beta\}$$

όλων των ζευγών εισόδων του T με διαφορά $\overline{\alpha}$ και εξοδοδιαφορά β. Ορίζουμε επίσης το σύνολο

$$\mathrm{IN}_T(\overline{\alpha}, \beta) = \{\overline{x} \mid (\exists \overline{x}^*)[(\overline{x}, \overline{x}^*) \in \Delta_T(\overline{\alpha}, \beta)]\}$$

όλων των πρώτων μελών των ζευγών του $\Delta_T(\overline{\alpha}, \beta)$ και συμβολίζουμε με

$$\mathrm{N}_T(\overline{\alpha}, \beta) = |\mathrm{IN}_T(\overline{\alpha}, \beta)|$$

το μέγεθός του.

4.2. Παρατηρηση. Είναι μια εύκολη διαπίστωση ότι το σύνολο $\mathrm{IN}_T(\overline{\alpha}, \beta)$ των πρώτων μελών των ζευγών του $\Delta_T(\overline{\alpha}, \beta)$ ταυτίζεται με το σύνολο των δεύτερων μελών του (αφού $(\overline{x}, \overline{x}^*) \in \Delta_T(\overline{\alpha}, \beta) \Longrightarrow (\overline{x}^*, \overline{x}) \in \Delta_T(\overline{\alpha}, \beta)$) και ότι μια πιο σύντομη περιγραφή και για τα δύο σύνολα είναι η

$$\mathrm{IN}_T(\overline{\alpha}, \beta) = \{\overline{x} \mid T(\overline{x}) \oplus T(\overline{x} \oplus \overline{\alpha}) = \beta\}.$$

Δηλαδή *ένα $\overline{x}$ ανήκει στο $\mathrm{IN}_T(\overline{\alpha}, \beta)$ αν και μόνο αν αυτό και το κατά $\overline{\alpha}$ διαφορετικό του έχουν εξοδοδιαφορά β ως προς τον T.*

Εξάλλου, είναι επίσης άμεσο ότι τα $\Delta_T(\overline{\alpha}, \beta)$ και $\mathrm{IN}_T(\overline{\alpha}, \beta)$ είναι ισοπληθικά, κι έτσι

$$\mathrm{N}_T(\overline{\alpha}, \beta) = |\mathrm{IN}_T(\overline{\alpha}, \beta)| = |\Delta_T(\overline{\alpha}, \beta)|.$$

Ο πίνακας που συνιστούν οι ποσότητες $\mathrm{N}_T(\overline{\alpha}, \beta)$ για όλα τα δυνατά $\overline{\alpha}$ και β είναι βεβαίως αυτός για τον οποίον μιλήσαμε πιο πάνω, και τον οποίον ονομάζουμε *πίνακα κατανομής διαφορών* (difference distribution table) του τελεστή T. Για παράδειγμα, οι πίνακες κατανομής διαφορών των συναρτήσεων αντικατάστασης $\alpha_{S_1'}, \ldots, \alpha_{S_8'}$ του DES είναι οι Πίνακες 3–10 του Παραρτήματος.

Τώρα είμαστε έτοιμοι να ορίσουμε την έννοια που θα μας επιτρέπει να προβλέπουμε εξοδοδιαφορές.

4.3. Ορισμος. Ονομάζουμε *διαφορική συμπεριφορά* του τυχόντος τελεστή $T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \to \mathbb{B}^n$ τη συνάρτηση

$$\delta_T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \times \mathbb{B}^n \to [0, 1]$$

που για κάθε διαφορά $\overline{\alpha}$ στοιχείων από το $\mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda}$ και κάθε διαφορά β στοιχείων από το $\mathbb{B}^n$ επιστρέφει την δεσμευμένη πιθανότητα

$$\delta_T(\overline{\alpha}, \beta) = \mathrm{Prob}[T(\overline{x}) \oplus T(\overline{x}^*) = \beta \mid \overline{x} \oplus \overline{x}^* = \overline{\alpha}]$$

ότι δύο ομοιόμορφα τυχαίες είσοδοι που διαφέρουν κατά $\overline{\alpha}$ θα έχουν εξοδοδιαφορά β ως προς τον τελεστή T.

Είναι φανερό ότι δεδομένου του πίνακα κατανομής διαφορών του T, ο υπολογισμός της διαφορικής του συμπεριφοράς είναι άμεσος.

4.4. Προταση. *Η διαφορική συμπεριφορά του τελεστή T του προηγούμενου ορισμού δίνεται από τον τύπο*

$$\delta_T(\overline{\alpha}, \beta) = \frac{\mathrm{N}_T(\overline{\alpha}, \beta)}{2^{n_1 + \cdots + n_\lambda}}.$$

Απόδειξη. Ο παρονομαστής είναι το πλήθος όλων των δυνατών ζευγαριών εισόδων που μπορούν να έχουν διαφορά $\overline{\alpha}$. Και ο αριθμητής το πλήθος εκείνων από αυτά τα ζευγάρια που έχουν εξοδοδιαφορά β. Η ισότητα ισχύει γιατί υποθέσαμε ότι τα ζευγάρια διαλέγονται ομοιόμορφα τυχαία. $\dashv$

Για παράδειγμα, η διαφορική συμπεριφορά των συναρτήσεων αντικατάστασης $\alpha_{S'_1}, \dots, \alpha_{S'_8}$ του DES προκύπτουν από τους Πίνακες 3–10 του Παραρτήματος, αν διαιρέσουμε κάθε τιμή με το πλήθος όλων των ζευγαριών εξάδων που έχουν τη διαφορά που αντιστοιχεί στη γραμμή, δηλαδή 64. Αναλυτικά,

$$\delta_{\alpha_{S'_j}}(\alpha, \beta) = \tfrac{1}{64}\mathrm{N}_{\alpha_{S'_j}}(\alpha, \beta), \tag{12}$$

για κάθε $\alpha \in \mathbb{B}^6$, και κάθε $\beta \in \mathbb{B}^4$.

Είναι σημαντικό να παρατηρήσουμε πως σε ό,τι ορίσαμε μέχρι στιγμής για τον τυχόντα τελεστή δεν προϋποθέσαμε ότι αυτός είναι διαφορικά μη αιτιοκρατικός. Οι ποσσότητες ορίζονται λοιπόν και για δ. αιτιοκρατικούς τελεστές, μόνο που παίρνουν τετριμμένες τιμές.

4.5. Πρόταση. *Αν ο τελεστής* $T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \to \mathbb{B}^n$ *είναι διαφορικά αιτιοκρατικός, τότε για κάθε διαφορά* $\overline{\alpha}$ *στοιχείων από το* $\mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda}$ *και κάθε διαφορά* β *στοιχείων από το* $\mathbb{B}^n$ *είναι*

$$\mathrm{N}_T(\overline{\alpha}, \beta) = \begin{cases} 2^{n_1 + \cdots + n_\lambda} & \textit{αν } \beta = \sigma_T(\overline{\alpha}), \\ 0 & \textit{αλλιώς,} \end{cases}$$

όπου σ_T *το διαφορικό αντίστοιχο του* T. *Οπότε και*

$$\delta_T(\overline{\alpha}, \beta) = \begin{cases} 1 & \textit{αν } \beta = \sigma_T(\overline{\alpha}), \\ 0 & \textit{αλλιώς.} \end{cases}$$

Απόδειξη. Άμεση από τους ορισμούς. $\dashv$

Τώρα εξετάζουμε πώς συμπεριφέρεται διαφορικά η σύνθεση τελεστών.

4.6. Πρόταση. *Ας είναι*

$$T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \to \mathbb{B}^n, \ \textit{και}$$
$$T_i : \mathbb{B}^{m_1} \times \cdots \times \mathbb{B}^{m_\varkappa} \to \mathbb{B}^{n_i} \qquad (1 \le i \le \lambda)$$

τυχόντες τελεστές. Με κάποια μη τετριμμένη παραδοχή, *η διαφορική συμπεριφορά της σύνθεσής τους*

$$U : \mathbb{B}^{m_1} \times \cdots \times \mathbb{B}^{m_\varkappa} \to \mathbb{B}^n, \ \textit{με}$$
$$U(x_1, \dots, x_\varkappa) = T\big(T_1(x_1, \dots, x_\varkappa), \dots, T_\lambda(x_1, \dots, x_\varkappa)\big)$$

είναι η συνάρτηση $\delta_U : \mathbb{B}^{m_1} \times \cdots \times \mathbb{B}^{m_\varkappa} \times \mathbb{B}^n \to [0,1]$ *που για κάθε διαφορά* $\overline{\alpha}$ *στοιχείων του* $\mathbb{B}^{m_1} \times \cdots \times \mathbb{B}^{m_\varkappa}$ *και κάθε διαφορά* β *στοιχείων του* $\mathbb{B}^n$ *επιστρέφει την τιμή*

$$\delta_U(\overline{\alpha}, \beta) = \sum_{\gamma_1 \in \mathbb{B}^{n_1}} \cdots \sum_{\gamma_\lambda \in \mathbb{B}^{n_\lambda}} \delta_{T_1}(\overline{\alpha}, \gamma_1) \cdots \delta_{T_\lambda}(\overline{\alpha}, \gamma_\lambda) \delta_T\big((\gamma_1, \dots, \gamma_\lambda), \beta\big). \tag{13}$$

Απόδειξη. Κατ' αρχήν θεωρούμε τα ενδεχόμενα

$$\begin{aligned} A &\iff \overline{x} \oplus \overline{x}^* = \overline{\alpha}, \\ B &\iff U(\overline{x}) \oplus U(\overline{x}^*) = \beta, \\ \Gamma_i(\gamma_i) &\iff T_i(\overline{x}) \oplus T_i(\overline{x}^*) = \gamma_i \qquad (i = 1, \ldots, \lambda \text{ και } \gamma_i \in \mathbb{B}^{n_i}). \end{aligned}$$

Ώστε, $\delta_U(\overline{\alpha}, \beta) = \mathrm{Prob}[B \mid A]$. (Βλέπε και Σχήμα 5.)

Από τη διαμέριση $\{\Gamma_1(\gamma_1) \mid \gamma_1 \in \mathbb{B}^{n_1}\}$ του δειγματοχώρου και το θεώρημα ολικής πιθανότητας έχουμε

$$\delta_U(\overline{\alpha}, \beta) = \mathrm{Prob}[B \mid A] = \sum_{\gamma_1 \in \mathbb{B}^{n_1}} \mathrm{Prob}[\Gamma_1(\gamma_1) \mid A] \cdot \mathrm{Prob}[B \mid \Gamma_1(\gamma_1) \wedge A].$$

Αλλά ο πρώτος παράγοντας σε κάθε γινόμενο είναι η τιμή $\delta_{T_1}(\overline{\alpha}, \gamma_1)$, άρα

$$\delta_U(\overline{\alpha}, \beta) = \sum_{\gamma_1 \in \mathbb{B}^{n_1}} \delta_{T_1}(\overline{\alpha}, \gamma_1) \mathrm{Prob}[B \mid \Gamma_1(\gamma_1) \wedge A].$$

Τώρα κάνουμε το ίδιο με την πιθανότητα που εμφανίζεται ως δεύτερος όρος σε κάθε γινόμενο και με τη διαμέριση $\{\Gamma_2(\gamma_2) \mid \gamma_2 \in \mathbb{B}^{n_2}\}$. Προκύπτει ότι

$$\mathrm{Prob}[B \mid \Gamma_1(\gamma_1) \wedge A] = \sum_{\gamma_2 \in \mathbb{B}^{n_2}} \delta_{T_2}(\overline{\alpha}, \gamma_2) \mathrm{Prob}[B \mid \Gamma_1(\gamma_1) \wedge \Gamma_2(\gamma_2) \wedge A],$$

επομένως και ότι

$$\delta_U(\overline{\alpha}, \beta) = \sum_{\gamma_1 \in \mathbb{B}^{n_1}} \sum_{\gamma_2 \in \mathbb{B}^{n_2}} \delta_{T_1}(\overline{\alpha}, \gamma_1) \delta_{T_2}(\overline{\alpha}, \gamma_2) \mathrm{Prob}[B \mid \Gamma_1(\gamma_1) \wedge \Gamma_2(\gamma_2) \wedge A].$$

Συνεχίζοντας με τον ίδιο τρόπο και αφού έχουμε χρησιμοποιήσει όλες τις διαμερίσεις, καταλήγουμε στο ότι

$$\begin{aligned} (14) \quad \delta_U(\overline{\alpha}, \beta) = \sum_{\gamma_1 \in \mathbb{B}^{n_1}} \cdots \sum_{\gamma_\lambda \in \mathbb{B}^{n_\lambda}} & \delta_{T_1}(\overline{\alpha}, \gamma_1) \cdots \delta_{T_\lambda}(\overline{\alpha}, \gamma_\lambda) \\ & \cdot \mathrm{Prob}[B \mid \Gamma_1(\gamma_1) \wedge \cdots \wedge \Gamma_\lambda(\gamma_\lambda) \wedge A], \end{aligned}$$

όπου ο τελευταίος παράγοντας κάθε γινομένου γράφεται απλούστερα ως

$$\mathrm{Prob}[B \mid \Gamma_1(\gamma_1) \wedge \cdots \wedge \Gamma_\lambda(\gamma_\lambda)]. \tag{15}$$

Τώρα υποθέτουμε ότι *καθώς τα ζευγάρια $(\overline{x}, \overline{x}^*)$ επιλέγονται ομοιόμορφα τυχαία μέσα από το σύνολο όλων των ζευγαριών με διαφορά $\overline{\alpha}$, το ζευγάρι*

$$\Big(\big(T_1(\overline{x}), \ldots, T_\lambda(\overline{x})\big), \big(T_1(\overline{x}^*), \ldots, T_\lambda(\overline{x}^*)\big) \Big)$$

των εισόδων του τελεστή T κινείται επίσης ομοιόμορφα τυχαία μέσα στο σύνολο των ζευγαριών που έχουν διαφορά $(\gamma_1, \ldots, \gamma_\lambda)$. Αν πράγματι συμβαίνει αυτό, τότε η πιθανότητα (15) είναι ακριβώς η $\delta_T\big((\gamma_1, \ldots, \gamma_\lambda), \beta\big)$. Οπότε η (14) δίνει άμεσα την (13). ⊣

4.7. Παρατηρηση. Εξηγούμε περισσότερο την μη τετριμμένη παραδοχή που ζητάει η εκφώνηση της προηγούμενης πρότασης.

Στην τελευταία παράγραφο της απόδειξης, θέλουμε να ισχύει ότι

$$\delta_T\big((\gamma_1, \ldots, \gamma_\lambda), \beta\big) = \mathrm{Prob}[B \mid \Gamma_1(\gamma_1) \wedge \cdots \wedge \Gamma_\lambda(\gamma_\lambda)].$$

Εύκολα, και τα δύο μέλη αναφέρονται στο ίδιο ακριβώς ενδεχόμενο: οι έξοδοι του τελεστή T (Σχήμα 5) να έχουν διαφορά β, όταν οι είσοδοί του έχουν διαφορά

$(\gamma_1, \ldots, \gamma_\lambda)$. Όμως, το δεύτερο μέλος είναι η πιθανότητα αυτού του ενδεχομένου πάνω από την ομοιόμορφα τυχαία επιλογή των ζευγών εισόδων του U μέσα από το σύνολο

$$\{(\overline{x}, \overline{x}^*) \mid \overline{x} \oplus \overline{x}^* = \overline{\alpha}\}$$

όλων των ζευγών με διαφορά $\overline{\alpha}$. Αντίθετα, το πρώτο μέλος είναι η πιθανότητα του ενδεχομένου πάνω από την ομοιόμορφα τυχαία επιλογή των ζευγών εισόδων του τελεστή T μέσα από το σύνολο

$$\{(\overline{y}, \overline{y}^*) \mid \overline{y} \oplus \overline{y}^* = (\gamma_1, \ldots, \gamma_\lambda)\}$$

όλων των ζευγών που έχουν διαφορά $(\gamma_1, \ldots, \gamma_\lambda)$. Για να ισχύει η ισότητα, αρκεί ο τρόπος επιλογής των εισόδων του U που απαιτεί το δεύτερο μέλος να συνεπάγεται ότι οι είσοδοι του T (έξοδοι των $T_1, \ldots, T_\lambda$) πράγματι παράγονται όπως απαιτεί το πρώτο μέλος. Αλλά αυτό δεν ισχύει πάντα· ένα εύκολο αντιπαράδειγμα είναι η περίπτωση που κάποιος από τους $T_1, \ldots, T_\lambda$ είναι σταθερός.

Επομένως, η υπόθεση που γίνεται στην τελευταία παράγραφο της απόδειξης είναι ουσιαστική. Και θα ισχύει (προσεγγιστικά, τουλάχιστον) σε όλες τις περιπτώσεις που πρόκειται να εφαρμόσουμε την Πρόταση 4.6.

Λαμβάνοντας υπόψη την Πρόταση 4.5, παίρνουμε δύο εύκολα πορίσματα για αντίστοιχες συχνές ειδικές περιπτώσεις σύνθεσης.

4.8. Πόρισμα. *Αν στην Πρόταση* 4.6 *οι τελεστές* $T_1, \ldots, T_\lambda$ *είναι όλοι τους διαφορικά αιτιοκρατικοί, τότε*

$$\delta_U(\overline{\alpha}, \beta) = \delta_T\Big(\big(\sigma_{T_1}(\overline{\alpha}), \ldots, \sigma_{T_\lambda}(\overline{\alpha})\big), \beta\Big).$$

4.9. Πόρισμα. *Αν στην Πρόταση* 4.6 *ο τελεστής* T *είναι διαφορικά αιτιοκρατικός, τότε*

$$\delta_U(\overline{\alpha}, \beta) = \sum_{\substack{\gamma_1 \in \mathbb{B}^{n_1}, \ldots, \gamma_\lambda \in \mathbb{B}^{n_\lambda} \\ \text{και } \sigma_T(\gamma_1, \ldots, \gamma_\lambda) = \beta}} \delta_{T_1}(\overline{\alpha}, \gamma_1) \cdots \delta_{T_\lambda}(\overline{\alpha}, \gamma_\lambda).$$

5. Διαφορική συμπεριφορά του DES

Τώρα θα υπολογίσουμε τη διαφορική συμπεριφορά της συνάρτησης κρυπτογράφησης e_k (Εξίσωση (1)).

Ξεκινάμε με τον τελεστή S. Από την Εξίσωση (2) της σελίδας 21 ξέρουμε ότι

$$S = \| \circ (h_1, \ldots, h_8), \qquad \text{με} \quad h_j = \alpha_{S_j} \circ \varepsilon_Z \circ \cdot_{(j)} = \alpha_{S'_j} \circ \cdot_{(j)},$$

για κάθε $j = 1, \ldots, 8$. Χρησιμοποιώντας το Πόρισμα 4.8 και την Εξίσωση (12), παίρνουμε για κάθε $j = 1, \ldots, 8$, κάθε $\alpha \in \mathbb{B}^{48}$ και κάθε $\beta \in \mathbb{B}^{32}$ ότι

$$\delta_{h_j}(\alpha, \beta) = \delta_{\alpha_{S'_j}}(\alpha_{(j)}, \beta) = \tfrac{1}{64} \mathrm{N}_{\alpha_{S'_j}}(\alpha_{(j)}, \beta).$$

Τώρα, με το Πόρισμα 4.9, παίρνουμε ότι

$$\delta_S(\alpha, \beta) = \sum_{\substack{\gamma_1 \in \mathbb{B}^6, \ldots, \gamma_8 \in \mathbb{B}^6 \\ \gamma_1 \| \cdots \| \gamma_8 = \beta}} \delta_{h_1}(\alpha, \gamma_1) \cdots \delta_{h_8}(\alpha, \gamma_8) = \delta_{h_1}(\alpha, \beta_{(1)}) \cdots \delta_{h_8}(\alpha, \beta_{(8)})$$

κι έτσι ότι τελικά

$$\delta_S(\alpha, \beta) = \frac{1}{2^{48}} \prod_{j=1}^{8} \mathrm{N}_{\alpha_{S'_j}}(\alpha_{(j)}, \beta_{(j)}), \qquad \text{για κάθε } \alpha \in \mathbb{B}^{48}, \beta \in \mathbb{B}^{32}. \tag{16}$$

Τώρα συνεχίζουμε για τον υπολογισμό της συμπεριφοράς της παραμετρικής εκδοχής F_v της συνάρτησης F, για το τυχόν υποκλειδί $v \in \mathbb{B}^{48}$. Ξέρουμε (Εξίσωση (1), σελίδα 19) ότι

$$F_v = \varepsilon_P \circ S \circ h, \qquad \text{όπου} \quad h = \oplus_v \circ \varepsilon_E.$$

Προφανώς, ο τελεστής h είναι δ. αιτιοκρατικός και $\sigma_h = \sigma_{\oplus_v} \circ \sigma_{\varepsilon_E} = \mathrm{i} \circ \varepsilon_E = \varepsilon_E$. Επομένως, από το Πόρισμα 4.8, είναι

$$\delta_{S \circ h}(\alpha, \beta) = \delta_S\big(\sigma_h(\alpha), \beta\big) = \delta_S\big(\varepsilon_E(\alpha), \beta\big),$$

για κάθε $\alpha, \beta \in \mathbb{B}^{32}$. Κι έτσι, από το Πόρισμα 4.9 κι επειδή $\sigma_{\varepsilon_P} = \varepsilon_P$, έχουμε, πάλι για κάθε $\alpha, \beta \in \mathbb{B}^{32}$,

$$\begin{aligned}\delta_{F_v}(\alpha, \beta) &= \sum_{\gamma \in \mathbb{B}^{32}, \varepsilon_P(\gamma) = \beta} \delta_{S \circ h}(\alpha, \gamma) = \delta_{S \circ h}\big(\alpha, \varepsilon_P^{-1}(\beta)\big) \\ &= \delta_S\big(\varepsilon_E(\alpha), \varepsilon_P^{-1}(\beta)\big) = \frac{1}{2^{48}} \prod_{j=1}^{8} \mathrm{N}_{\alpha_{S'_j}}\big(\varepsilon_E(\alpha)_{(j)}, \varepsilon_P^{-1}(\beta)_{(j)}\big).\end{aligned}$$

Τελικά, χρησιμοποιώντας τις συντομογραφίες του Ορισμού 1.1, παίρνουμε ότι

$$\delta_{F_v}(\alpha, \beta) = \frac{1}{2^{48}} \prod_{j=1}^{8} \mathrm{N}_{\alpha_{S'_j}}(\alpha_{\langle j \rangle}, \beta_{[j]}), \qquad \text{για κάθε } \alpha, \beta \in \mathbb{B}^{32}. \tag{17}$$

Για να υπολογίσουμε τη διαφορική συμπεριφορά μιας Feistel μετάθεσης της e_k, έστω f_v για το τυχόν υποκλειδί $v \in \mathbb{B}^{48}$, πρώτα θυμόμαστε (Ορισμός 1-3.4) ότι

$$f_v = \| \circ \big(\cdot^R, g_v\big), \qquad \text{όπου} \quad g_v = \oplus \circ (\cdot^L, F_v \circ \cdot^R).$$

Προφανώς, για κάθε $\alpha \in \mathbb{B}^{64}$ και $\beta \in \mathbb{B}^{32}$, είναι $\delta_{F_v \circ \cdot^R}(\alpha, \beta) = \delta_{F_v}(\alpha^R, \beta)$, επομένως θα είναι

$$\delta_{g_v}(\alpha, \beta) = \sum_{\substack{\gamma_1, \gamma_2 \in \mathbb{B}^{32} \\ \gamma_1 \oplus \gamma_2 = \beta}} \delta_{\cdot^L}(\alpha, \gamma_1) \delta_{F_v \circ \cdot^R}(\alpha, \gamma_2) = \sum_{\gamma_1 \in \mathbb{B}^{32}} \delta_{\cdot^L}(\alpha, \gamma_1) \delta_{F_v}(\alpha^R, \gamma_1 \oplus \beta).$$

Αλλά (Πρόταση 4.5) ο πρώτος παράγοντας κάθε γινομένου είναι σταθερά 0, με μόνη εξαίρεση την περίπτωση που $\gamma_1 = \alpha^L$, οπότε είναι 1. Άρα

$$\delta_{g_v}(\alpha, \beta) = \delta_{F_v}(\alpha^R, \alpha^L \oplus \beta).$$

Τώρα υπολογίζουμε

$$\begin{aligned}\delta_{f_v}(\alpha, \beta) &= \sum_{\substack{\gamma_1, \gamma_2 \in \mathbb{B}^{3}2 \\ \gamma_1 \| \gamma_2 = \beta}} \delta_{\cdot^R}(\alpha, \gamma_1) \delta_{g_v}(\alpha, \gamma_2) = \delta_{\cdot^R}(\alpha, \beta^L) \delta_{g_v}(\alpha, \beta^R) \\ &= \delta_{\cdot^R}(\alpha, \beta^L) \delta_{F_v}(\alpha^R, \alpha^L \oplus \beta^R),\end{aligned}$$

όπου ο πρώτος παράγοντας είναι πάντα 0, εκτός από την περίπτωση $\alpha^R = \beta^L$, οπότε και γίνεται 1. Τελικά,

$$\delta_{f_v}(\alpha, \beta) = \begin{cases} 0 & \text{αν } \alpha^R \neq \beta^L, \\ \frac{1}{2^{48}} \prod_{j=1}^{8} \mathrm{N}_{\alpha_{S'_j}}\big((\alpha^R)_{\langle j \rangle}, (\alpha^L \oplus \beta^R)_{[j]}\big) & \text{αν } \alpha^R = \beta^L, \end{cases} \tag{18}$$

για κάθε $\alpha, \beta \in \mathbb{B}^{64}$.

Το επόμενο βήμα είναι να υπολογίσουμε τη διαφορική συμπεριφορά μιας Feistel διμετάθεσης, $a_{v,w} = f_w \circ f_v$, για τυχόντα υποκλειδιά $v, w \in \mathbb{B}^{48}$. Καθώς κανένας από τους δύο συντιθέμενους τελεστές δεν είναι δ. αιτιοκρατικός, χρησιμοποιούμε απ' ευθείας την Πρόταση 4.6 και παίρνουμε

$$\delta_{a_{v,w}} = \sum_{\gamma \in \mathbb{B}^{64}} \delta_{f_v}(\alpha,\gamma)\delta_{f_w}(\gamma,\beta).$$

Αλλά ο πρώτος παράγοντας κάθε γινομένου είναι μη μηδενικός μόνο όταν $\alpha^R = \gamma^L$. Παρόμοια, ο δεύτερος παράγοντας κάθε γινομένου είναι μη μηδενικός μόνο όταν $\gamma^R = \beta^L$. Επομένως, το μόνο μη μηδενικό γινόμενο είναι αυτό που αντιστοιχεί στην περίπτωση $\alpha^R = \gamma^L \wedge \gamma^R = \beta^L$, δηλαδή στην $\gamma = \alpha^R \,\|\, \beta^L$. Άρα

$$\delta_{a_{v,w}} = \delta_{f_v}(\alpha, \alpha^R \,\|\, \beta^L)\delta_{f_w}(\alpha^R \,\|\, \beta^L, \beta),$$

και μετά από λίγες πράξεις

$$\delta_1(\alpha,\beta) = \frac{1}{2^{96}} \prod_{j=1}^{8} \mathrm{N}_{\alpha_{S'_j}}\big((\alpha^R)_{\langle j\rangle}, (\alpha^L \oplus \beta^L)_{[j]}\big) \cdot \mathrm{N}_{\alpha_{S'_j}}\big((\beta^L)_{\langle j\rangle}, (\alpha^R \oplus \beta^L)_{[j]}\big), \tag{19}$$

για κάθε $\alpha, \beta \in \mathbb{B}^{64}$.

5.1. Παρατηρηση. Όπως φαίνεται από την (19), η διαφορική συμπεριφορά μιας Feistel διμετάθεσης του DES *δεν* εξαρτάται από τα υποκλειδιά που χρησιμοποιούνται στις δύο συντιθέμενες Feistel μεταθέσεις, κι επομένως δεν εξαρτάται καθόλου από το κλειδί. Αυτό φάνηκε ήδη από την (17) και μετά από την (18), όπου επίσης το υποκλειδί δεν είχε καμιά επιρροή.

Τώρα είναι ένα τετριμμένο επαγωγικό επιχείρημα να δείξουμε ότι η διαφορική συμπεριφορά δ_s της σύνθεσης s Feistel διμεταθέσεων δίνεται από τον τύπο

$$\delta_s(\alpha,\beta) = \sum_{\gamma_1 \in \mathbb{B}^{64}} \cdots \sum_{\gamma_{s-1} \in \mathbb{B}^{64}} \delta_1(\alpha,\gamma_1)\delta_1(\gamma_1,\gamma_2)\cdots\delta_1(\gamma_{s-1},\beta), \tag{20}$$

για κάθε $\alpha, \beta \in \mathbb{B}^{64}$. Αν λοιπόν υποθέσουμε ότι το πλήθος r των Feistel γύρων της συνάρτησης κρυπτογράφησης e_k είναι άρτιο, τότε υπάρχουν $\frac{r}{2}$ Feistel διμεταθέσεις κι έτσι η συμπεριφορά της e_k δίνεται από τον παραπάνω τύπο για $s = \frac{r}{2}$.

6. Η τεχνική (συνέχεια)

Τώρα μπορούμε να συνεχίσουμε την περιγραφή της βασικής ιδέας από το σημείο στο οποίο την αφήσαμε στο τέλος της Ενότητας 2. Είχαμε αποφασίσει ότι θα πρέπει να βρούμε κάποιες διαφορές πακέτων $\alpha, \beta \in \mathbb{B}^{64}$ τέτοιες που, όταν διαλέγουμε στην είσοδο ζευγάρια κειμένων (p, p^*) ομοιόμορφα και τυχαία μέσα από το σύνολο

$$\{(p,p^*) \mid p \oplus p^* = \alpha\},$$

η διαφορά των αντίστοιχων εισόδων (z_{r-2}, z^*_{r-2}) του προτελευταίου Feistel γύρου της συνάρτησης κρυπτογράφησης να γίνεται β, με κάποια πιθανότητα π.

Όμως η διαφορά $z_{r-2} \oplus z^*_{r-2}$ δεν είναι παρά η εξοδοδιαφορά των p και p^* ως προς τη σύνθεση 7 Feistel διμεταθέσεων (14 Feistel μεταθέσεων). Οπότε, η πιθανότητα π δεν είναι παρά η τιμή της διαφορικής συμπεριφοράς αυτής της σύνθεσης για το ζευγάρι διαφορών (α, β). Δηλαδή, σύμφωνα και με την Εξίσωση (20) για $s = 7$,

$$\pi = \delta_7(\alpha,\beta) = \sum_{\gamma_1 \in \mathbb{B}^{64}} \cdots \sum_{\gamma_6 \in \mathbb{B}^{64}} \delta_1(\alpha,\gamma_1)\delta_1(\gamma_1,\gamma_2)\cdots\delta_1(\gamma_6,\beta),$$

με δ_1 βεβαίως τη διαφορική συμπεριφορά της μίας Feistel διμετάθεσης, από την Εξίσωση (19).

Όπως ήδη έχουμε εξηγήσει, για να καταστήσουμε τον Αλγόριθμο 2 (σελίδα 57) ικανό να προσβάλλει το DES, είναι κρίσιμο να κάνουμε την π όσο το δυνατόν μεγαλύτερη· ισοδύναμα, να βρούμε $\alpha, \beta \in \mathbb{B}^{64}$ τέτοια που να μεγιστοποιούν την τιμή $\delta_7(\alpha, \beta)$. Όμως αυτό δεν είναι εύκολο, καθώς η δ_7 δεν έχει αναλυτικό τύπο που να επιτρέπει τη μελέτη ακροτάτων, ενώ η εξαντλητική εύρεση του μεγίστου απαιτεί το απαγορευτικό πλήθος των $|\mathbb{B}^{64} \times \mathbb{B}^{64}| = 2^{128}$ συγκρίσεων. Και το χειρότερο: ακόμη και ο υπολογισμός της τιμής $\delta_7(\alpha, \beta)$ για μόνο ένα ζευγάρι (α, β) είναι επίσης απαγορευτικά ακριβός, αφού απαιτεί την άθροιση $|\mathbb{B}^{64}|^6 = 2^{384}$ γινομένων.

Γι' αυτό το δεύτερο πρόβλημα, του υπολογισμού της τιμής $\delta_7(\alpha, \beta)$ για κάποια συγκεκριμένα α και β, δεν έχουμε λύση. Θεωρούμε λοιπόν επιτυχία ακόμη και το να βρούμε ένα καλό κάτω φράγμα αυτής της τιμής. Βεβαίως, ως άθροισμα θετικών όρων της μορφής

$$\delta_1(\alpha, \gamma_1)\delta_1(\gamma_1, \gamma_2) \cdots \delta_1(\gamma_6, \beta), \tag{21}$$

η τιμή $\delta_7(\alpha, \beta)$ κάτω φράσσεται από καθένα από αυτούς τους όρους. Και κάθε τέτοιος όρος καθορίζεται πλήρως από τις τιμές $\gamma_1, \ldots, \gamma_6$. Επομένως, υποχωρούμε τελικά στο να προσπαθούμε να βρούμε με ευριστικό τρόπο μια εξάδα τιμών $\gamma_1, \ldots, \gamma_6$ που να κάνει το γινόμενο (21) όσο το δυνατόν μεγαλύτερο.

Έτσι, το πρώτο πρόβλημα, της εύρεσης του μέγιστου της δ_7, προσπαθούμε να το λύσουμε με δεδομένα όχι τις ίδιες τις τιμές $\delta_7(\alpha, \beta)$ για όλα τα $\alpha, \beta \in \mathbb{B}^{64}$, αλλά τα αντίστοιχα υπολογισμένα κάτω φράγματα. Όμως και τότε, το πλήθος των τιμών που πρέπει να συγκρίνουμε εξακολουθεί να είναι απαγορευτικά μεγάλο. Υποχωρούμε λοιπόν και πάλι μόνο στο να προσπαθούμε να βρούμε με ευριστικό τρόπο ένα ζευγάρι για το οποίο να είναι όσο το δυνατόν μεγαλύτερο το αντίστοιχο κάτω φράγμα.

Συνολικά, από το να ξέρουμε όλες τις τιμές της δ_7 και να βρούμε τη μέγιστη, έχουμε τελικά υποχωρήσει στο *να βρούμε μια ακολουθία τιμών* $\alpha = \gamma_0, \gamma_1, \ldots, \gamma_6$, $\gamma_7 = \beta$ *που να μεγιστοποιεί το γινόμενο* (21). Κάθε τέτοια ακολουθία τη λέμε *χαρακτηριστική* (characteristic). Η εύρεση χαρακτηριστικών με όσο το δυνατόν μεγαλύτερη πιθανότητα δεν είναι τετριμμένο πρόβλημα. Οι τεχνικές που χρησιμοποιούνται για τη λύση του εξαρτώνται σημαντικά από το υπο εξέταση κρυπτοσύστημα.

ΚΕΦΑΛΑΙΟ 5

Γραμμική κρυπτανάλυση

Η *γραμμική κρυπτανάλυση* (linear cryptanalysis) είναι μια μέθοδος επίθεσης με γνωστά κείμενα που έχει εφαρμοστεί με επιτυχία στο DES [**17, 16**], αλλά και σε άλλα κρυπτοσυστήματα με ανάλογα αποτελέσματα.

1. Συμβάσεις–συμβολισμοί

Η παρουσίαση της τεχνικής γίνεται πάνω στο DES. Για απλότητα, χρησιμοποιούμε τις συμβάσεις και τους συμβολισμούς της Ενότητας 4-1. Εισάγουμε και μερικές νέες έννοιες.

1.1. Ορισμος. Για το τυχόν $n \geq 1$ και κάθε $x, \alpha \in \mathbb{B}^n$ συμβολίζουμε με

$$x \cdot \alpha$$

τη *δυαδική σύζευξη* (bitwise and) των x και α. Γενικά, για κάθε $\lambda, n_1, \ldots, n_\lambda \geq 1$ και κάθε δύο $\overline{x} = (x_1, \ldots, x_\lambda), \overline{\alpha} = (\alpha_1, \ldots, \alpha_\lambda) \in \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda}$, θέτουμε

$$\overline{x} \cdot \overline{\alpha} = (x_1 \cdot \alpha_1, \ldots, x_\lambda \cdot \alpha_\lambda).$$

Επίσης, ονομάζουμε *ισοτιμία* (parity) της x το ψηφίο

$$\operatorname{par}(x) = \begin{cases} 0 & \text{αν η } x \text{ έχει άρτιο πλήθος από 1} \\ 1 & \text{αν η } x \text{ έχει περιττό πλήθος από 1,} \end{cases}$$

και ορίζουμε τα ψηφία $x[\alpha]$ και $\overline{x}[\overline{\alpha}]$ να είναι τα

$$x[\alpha] = \operatorname{par}(x \cdot \alpha), \qquad \overline{x}[\overline{\alpha}] = \bigoplus_{i=1}^{\lambda} \operatorname{par}(x_i \cdot \alpha_i).$$

Ο συμβολισμός $x[\alpha]$ είναι χρήσιμος για τον υπολογισμό της ισοτιμίας κάποιας υπακολουθίας x' της x. Αν διαλέξουμε την α να είναι η μοναδική ακολουθία με άσους ακριβώς στις θέσεις των ψηφίων της x' μέσα στη x, τότε $\operatorname{par}(x') = x[\alpha]$. Σε τέτοιες περιπτώσεις λέμε ότι η α είναι μια *μάσκα* για την επιλογή των ψηφίων της x'. Π.χ., για τον υπολογισμό της ισοτιμίας των ψηφίων των περιττών θέσεων μιας 8-ψήφιας ακολουθίας χρησιμοποιούμε τη μάσκα 10101010 ως εξής: $00110101[10101010] = \operatorname{par}(0100) = 1$.

2. Η τεχνική

Ας υποθέσουμε ότι έχουμε βρει κάποια $\alpha, \beta \in \mathbb{B}^{64}$ και $\gamma \in \mathbb{B}^{56} \setminus \{00\cdots0\}$ τέτοια ώστε, όταν το κείμενο p επιλέγεται ομοιόμορφα τυχαία μέσα από το σύνολο $\mathbb{B}^{56}$ όλων των κειμένων και $q \in \mathbb{B}^{64}$ είναι κάθε φορά το αντίστοιχο κρυπτοκείμενο, η εξίσωση

$$p[\alpha] \oplus q[\beta] = k[\gamma] \tag{1}$$

ισχύει με πιθανότητα π. Δηλαδή, με πιθανότητα π πάνω από την ομοιόμορφα τυχαία επιλογή του p, στα ψηφία του κλειδιού που διαλέγονται με τη μάσκα γ βρίσκουμε τόσους άσους (modulo 2) όσους και στα ψηφία που διαλέγονται από το κείμενο και το κρυπτοκείμενο με τις μάσκες α και β.

Το σημαντικό είναι ότι η (1) συνδέει το άγνωστο ψηφίο $k[\gamma]$ με το γνωστό ψηφίο $p[\alpha] \oplus q[\beta]$ —έχουμε υποθέσει επίθεση με γνωστά κείμενα, οπότε θεωρούμε ότι κάθε φορά τα p και q είναι γνωστά. Και αν μπορέσουμε να μάθουμε αυτό το άγνωστο ψηφίο, τότε είναι προφανές ότι έχουμε μειώσει στο μισό το χώρο αναζήτησης για το k.

Θέλουμε λοιπόν να χρησιμοποιήσουμε την εξίσωση (1) για να βρούμε το ψηφίο $k[\gamma]$. Η ιδέα για να το κάνουμε αυτό βασίζεται στη γνώση της πιθανότητας π: Αν ξέρουμε ότι $\pi > \frac{1}{2}$, τότε μπορούμε να διαλέξουμε N ομοιόμορφα τυχαία κείμενα $p_1, \ldots, p_N$, να υπολογίσουμε τα ψηφία

$$p_i[\alpha] \oplus q_i[\beta] \qquad (i = 1, \ldots, N)$$

και να περιμένουμε ότι τα περισσότερα από αυτά ($N\pi > \frac{N}{2}$) θα είναι ίσα με το $k[\gamma]$ —αφού στις περισσότερες από τις περιπτώσεις θα ισχύει η (1). Δηλαδή βρίσκουμε το $k[\gamma]$ με τον παρακάτω αλγόριθμο.

Αλγόριθμος 3

Είσοδος: Οι μάσκες $\alpha, \beta \in \mathbb{B}^{64}$ έτσι που η Εξίσωση (1) να ισχύει με $\pi > \frac{1}{2}$.
Έξοδος: Το ψηφίο $k[\gamma]$.
Μέθοδος: 0. Διάλεξε N κείμενα $p_1, \ldots, p_N$ ομοιόμορφα τυχαία μέσα από το $\mathbb{B}^{64}$. Ας είναι $q_1, \ldots, q_N$ τα αντίστοιχα κρυπτοκείμενα.
1. Θεώρησε 2 μετρητές, c_0 και c_1, με αρχική τιμή μηδέν.
2. Για κάθε $i = 1, \ldots, N$:
   2α. Υπολόγισε το ψηφίο $\psi = p_i[\alpha] \oplus q_i[\beta]$.
   2β. Αύξησε κατά 1 τον αντίστοιχο μετρητή, $c_\psi \longleftarrow c_\psi + 1$.
3. Αν $c_0 > c_1$, επέστρεψε 0. Αλλιώς, επέστρεψε 1.

Και μπορούμε να υπολογίσουμε την πιθανότητα ότι ο αλγόριθμος θα επιστρέψει πράγματι τη σωστή τιμή.

2.1. Πρόταση. *Αν $\pi > \frac{1}{2}$ είναι η πιθανότητα να ισχύει η Εξίσωση (1) και N είναι το πλήθος των κειμένων που διαλέγει ο Αλγόριθμος 3, τότε η επιστρεφόμενη τιμή του αλγορίθμου είναι ορθή με πιθανότητα*

$$\Phi\big(2\sqrt{N}(\pi - \tfrac{1}{2})\big),$$

όπου Φ η συνάρτηση κατανομής της τυποποιημένης κανονικής μεταβλητής.

Απόδειξη. Ο αλγόριθμος εκτελεί N ανεξάρτητες δοκιμές Bernoulli (τυχαία επιλογή ενός κειμένου p και έλεγχος του αν αυτό ικανοποιεί την (1)), με πιθανότητα επιτυχίας π κάθε φορά. Αν X είναι η τυχαία μεταβλητή που μετράει το πλήθος των επιτυχιών, τότε η τιμή που επιστρέφει ο αλγόριθμος είναι η σωστή αν και μόνο αν

$$X > \frac{N}{2}.$$

Προφανώς, η X έχει τη διωνυμική κατανομή, με παραμέτρους N και π. Αν το N είναι αρκετά μεγάλο, τότε μπορούμε να προσεγγίσουμε τη συνάρτηση κατανομής της

N	$\frac{1}{4}(\pi-\frac{1}{2})^{-2}$	$\frac{1}{2}(\pi-\frac{1}{2})^{-2}$	$(\pi-\frac{1}{2})^{-2}$	$2(\pi-\frac{1}{2})^{-2}$
Π	0.841	0.921	0.977	0.998

Πινακας 1. Η πιθανότητα Π ότι ο Αλγόριθμος 3 θα επιστρέψει τη σωστή τιμή, ως συνάρτηση της σχέσης του πλήθους N με την πιθανότητα π.

X με αυτήν της τυποποιημένης κανονικής μεταβλητής, ώστε έχουμε

$$\begin{aligned}\mathrm{Prob}\big[X > \tfrac{N}{2}\big] &= 1 - \mathrm{Prob}\big[X \leq \tfrac{N}{2}\big]\\ &\approx 1 - \Phi\Big(\frac{\frac{N}{2} - N\pi + \frac{1}{2}}{\sqrt{N}\sqrt{\pi(1-\pi)}}\Big)\\ &\approx 1 - \Phi\big(-2\sqrt{N}(\pi - \tfrac{1}{2})\big)\\ &= \Phi\big(2\sqrt{N}(\pi - \tfrac{1}{2})\big),\end{aligned}$$

το ζητούμενο. ⊣

Επομένως, η πιθανότητα να πάρουμε τη σωστή τιμή μεγαλώνει όσο περισσότερο μεγαλώνουν τα N και $\pi \in (\frac{1}{2}, 1]$. Αλλά συνήθως η τιμή του π είναι δεδομένη· καθορίζεται από το κρυπτοσύστημα και από το πόσο καλά έχουμε ψάξει για να βρούμε εξισώσεις σαν την (1). Οπότε, για να ελέγξουμε την παραπάνω πιθανότητα μας μένει να μεταβάλουμε το πλήθος N. Ο Πίνακας 1 δείχνει τι περίπου συμβαίνει καθώς το πλήθος N αλλάζει τη σχέση του ως προς την πιθανότητα π. Για $N = \frac{2}{(\pi-1/2)^2}$ ο αλγόριθμος είναι σχεδόν βέβαια ορθός.

Από αυτό φαίνεται ότι γενικά θέλουμε να έχουμε βρει τέτοιες μάσκες $\alpha, \beta \in \mathbb{B}^{64}$ και $\gamma \in \mathbb{B}^{56}$, ώστε η πιθανότητα $\pi > \frac{1}{2}$ με την οποία ισχύει η Εξίσωση (1) να είναι όσο το δυνατόν πιο κοντά στο 1, για να είναι και το αναγκαίο πλήθος N όσο το δυνατόν μικρότερο. Αλλά μια εξίσωση σαν την (1) μπορούμε να την εκμεταλλευτούμε ακόμη και όταν $\pi < \frac{1}{2}$.

Πράγματι, αν η (1) ισχύει με πιθανότητα $\pi < \frac{1}{2}$, τότε η εξίσωση

$$\overline{p[\alpha] \oplus q[\beta]} = k[\gamma] \tag{2}$$

εκφράζει το ακριβώς συμπληρωματικό γεγονός και επομένως ισχύει με πιθανότητα $1 - \pi > \frac{1}{2}$. Οπότε, μπορούμε και πάλι να εφαρμόσουμε τον Αλγόριθμο 3, τροποποιώντας μόνο το Βήμα 2α, στο 2α′.

Αλγόριθμος 3′

...

2α′. Υπολόγισε το ψηφίο $\psi = \overline{p[\alpha] \oplus q[\beta]}$.

...

Και, σ' αυτήν την περίπτωση, το πλήθος N γίνεται τόσο μικρότερο όσο πιο πολύ πλησιάζει το π στο 0.

Από τα παραπάνω γίνεται σαφές ότι η χρησιμότητα μιας εξίσωσης σαν την (1) είναι τόσο μεγαλύτερη όσο πιο μακριά από το $\frac{1}{2}$ είναι η πιθανότητα π με την οποία ισχύει, δηλαδή όσο πιο μεγάλο είναι το $|\pi - \frac{1}{2}|$.

Συνοψίζουμε τα παραπάνω στον ορισμό που ακολουθεί.

2.2. Ορισμος. Για κάθε $\alpha, \beta \in \mathbb{B}^{64}$ και κάθε $\gamma \in \mathbb{B}^{56}$ λέμε ότι η Εξίσωση (1) είναι μια *γραμμική προσέγγιση* (linear approximation) του DES. Αν αυτή ισχύει με πιθανότητα π πάνω από την ομοιόμορφα τυχαία επιλογή του p, τότε το

$$\epsilon = |\pi - \tfrac{1}{2}|$$

λέγεται *αποτελεσματικότητα* (effectiveness) της εξίσωσης.

Μένει λοιπόν να βρούμε μια γραμμική προσέγγιση του DES με όσο το δυνατόν μεγαλύτερη αποτελεσματικότητα.

3. Γραμμική συμπεριφορά τελεστή

Προκειμένου να συστηματοποιήσουμε την αναζήτηση της πιο αποτελεσματικής γραμμικής προσέγγισης του DES, γενικεύουμε το ζήτημα, ανάλογα προς την Ενότητα 4 του Κεφαλαίου 4. Το πρώτο βήμα είναι ο επόμενος ορισμός.

3.1. Ορισμος. Ας είναι $T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \to \mathbb{B}^{n}$ τυχών τελεστής. Για κάθε μάσκα $\overline{\alpha}$ στο $\mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda}$ και κάθε μάσκα β στο $\mathbb{B}^{n}$, ορίζουμε το σύνολο

$$\mathrm{IM}_T(\overline{\alpha}, \beta) = \{\overline{x} \mid \overline{x}[\overline{\alpha}] = T(\overline{x})[\beta]\}$$

όλων των εισόδων του T που, υπο τις επιλογές ψηφίων που ορίζουν οι μάσκες $\overline{\alpha}$ και β, παράγουν έξοδο με την ίδια ισοτιμία. Συμβολίζουμε με

$$\mathrm{M}_T(\overline{\alpha}, \beta) = |\mathrm{IM}_T(\overline{\alpha}, \beta)|$$

το μέγεθος αυτού του συνόλου.

Τον πίνακα που συνιστούν οι ποσότητες $\mathrm{M}_T(\overline{\alpha}, \beta)$ για όλα τα $\overline{\alpha}$ και β θα τον πούμε *πίνακα διατήρησης ισοτιμιών*. Παραδείγματα είναι οι Πίνακες 11–18 του Παραρτήματος.

3.2. Ορισμος. Ονομάζουμε *γραμμική συμπεριφορά* του τυχόντος τελεστή $T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \to \mathbb{B}^{n}$ τη συνάρτηση

$$\gamma_T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \times \mathbb{B}^{n} \to [0, 1]$$

που για κάθε μάσκα $\overline{\alpha}$ στο $\mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda}$ και κάθε μάσκα β στο $\mathbb{B}^{n}$, επιστρέφει την πιθανότητα

$$\gamma_T(\overline{\alpha}, \beta) = \mathrm{Prob}\Big[\overline{x}[\overline{\alpha}] = T(\overline{x})[\beta]\Big]$$

ότι μια ομοιόμορφα τυχαία είσοδος παράγει στην έξοδο την ίδια ισοτιμία, υπό τις επιλογές ψηφίων που ορίζουν οι $\overline{\alpha}$ και β.

Είναι προφανές ότι δεδομένου του πίνακα διατήρησης ισοτιμιών του T, ο υπολογισμός της γραμμικής του συμπεριφοράς είναι άμεσος.

3.3. Προταση. *Η γραμμική συμπεριφορά του τελεστή T του προηγούμενου ορισμού δίνεται από τον τύπο*

$$\gamma_T(\overline{\alpha}, \beta) = \frac{\mathrm{M}_T(\overline{\alpha}, \beta)}{2^{n_1 + \cdots + n_\lambda}}.$$

Αποδειξη. Ο παρονομαστής είναι το πλήθος όλων των δυνατών εισόδων στον T. Ο αριθμητής είναι το πλήθος των εισόδων που προκαλούν έξοδο με την ίδια ισοτιμία, υπό τις επιλογές ψηφίων που ορίζουν οι μάσκες $\overline{\alpha}$ και β. Η ισότητα ισχύει γιατί υποθέσαμε ότι οι είσοδοι επιλέγονται ομοιόμορφα τυχαία. $\dashv$

Για παράδειγμα, η γραμμική συμπεριφορά των συναρτήσεων αντικατάστασης $\alpha_{S'_1}, \ldots, \alpha_{S'_8}$ του DES προκύπτουν από τους Πίνακες 11–18 του Παραρτήματος, αν διαιρέσουμε κάθε τιμή με το πλήθος όλων των δυνατών εισόδων, δηλαδή με το 64. Αναλυτικά,

$$\gamma_{\alpha_{S'_j}}(\alpha, \beta) = \tfrac{1}{64}\mathrm{M}_{\alpha_{S'_j}}(\alpha, \beta), \tag{3}$$

για κάθε $\alpha \in \mathbb{B}^6$, και κάθε $\beta \in \mathbb{B}^4$.

Βεβαίως, όπως θα φανεί πιο κάτω, αυτό που μας ενδιαφέρει για τις τιμές της γραμμικής συμπεριφοράς ενός τελεστή δεν είναι το πόσο μεγάλες μπορούν να γίνουν, αλλά το πόσο μακριά από το $\frac{1}{2}$ μπορούν να βρεθούν. Για να κάνουμε τέτοιους είδους παρατηρήσεις, εισάγουμε την επόμενη έννοια.

3.4. Ορισμος. Ονομάζουμε *αποτελεσματικότητα* (effectiveness) του τυχόντος τελεστή $T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \to \mathbb{B}^n$ τη συνάρτηση

$$\epsilon_T : \mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda} \times \mathbb{B}^n \to \left[0, \tfrac{1}{2}\right]$$

που για κάθε μάσκα $\overline{\alpha}$ στο $\mathbb{B}^{n_1} \times \cdots \times \mathbb{B}^{n_\lambda}$ και κάθε μάσκα β στο $\mathbb{B}^n$, επιστρέφει την απόσταση

$$\epsilon_T(\overline{\alpha}, \beta) = \left|\gamma_T(\overline{\alpha}, \beta) - \tfrac{1}{2}\right|$$

της τιμής της γραμμικής συπεριφοράς από το $\frac{1}{2}$.

Τώρα μπορούμε από τη γραμμική συμπεριφορά δύο ή περισσότερων τελεστών να υπολογίσουμε τη γραμμική συμπεριφορά της σύνθεσής τους. Δυστυχώς, όπως θα σχολιάσουμε και παρακάτω, αυτό μπορεί να γίνει εύκολα μόνο στην περίπτωση που οι τελεστές είναι απλές μεταθέσεις.

3.5. Προταση. *Έστω $T_1 : \mathbb{B}^n \rightarrowtail\!\!\!\!\twoheadrightarrow \mathbb{B}^n$ και $T_2 : \mathbb{B}^n \rightarrowtail\!\!\!\!\twoheadrightarrow \mathbb{B}^n$ δύο μεταθέσεις του $\mathbb{B}^n$ και $T = T_2 \circ T_1$ η σύνθεσή τους. Η γραμμική συμπεριφορά του T είναι η συνάρτηση $\gamma_T : \mathbb{B}^n \times \mathbb{B}^n \to [0,1]$ που για κάθε δύο μάσκες $\alpha, \beta \in \mathbb{B}^n$ επιστρέφει την τιμή*

$$\gamma_T(\alpha, \beta) = 2\theta\gamma_{T_1}(\alpha, \gamma) + 1 - \gamma_{T_1}(\alpha, \gamma) - \gamma_{T_2}(\gamma, \beta).$$

Ως γ μπορούμε να διαλέξουμε οποιαδήποτε μάσκα στο $\mathbb{B}^n$ και τότε το θ είναι η δεσμευμένη πιθανότητα

$$\theta = \mathrm{Prob}\Big[T_1(x)[\gamma] = T_2\big(T_1(x)\big)[\beta] \;\Big|\; x[\alpha] = T_1(x)[\gamma]\Big], \tag{4}$$

όταν το x διαλέγεται ομοιόμορφα τυχαία μέσα από το $\mathbb{B}^n$. (Σχήμα 1.)

Αποδειξη. Ας είναι α και β δύο οποιεσδήποτε μάσκες στο $\mathbb{B}^n$. Για να υπολογίσουμε την τιμή

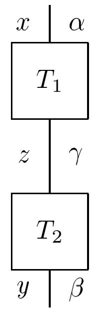
$$\gamma_T(\alpha, \beta) = \mathrm{Prob}\Big[x[\alpha] = T(x)[\beta]\Big] = \mathrm{Prob}\Big[x[\alpha] = T_2\big(T_1(x)\big)[\beta]\Big],$$

(με την πιθανότητα να υπολογίζεται όταν το x διαλέγεται ομοιόμορφα τυχαία μέσα από το $\mathbb{B}^n$) επιλέγουμε μια οποιαδήποτε μάσκα γ από το $\mathbb{B}^n$ και παρατηρούμε ότι

- όταν το x επιλέγεται ομοιόμορφα τυχαία μέσα από το $\mathbb{B}^n$, η εξίσωση

  $$x[\alpha] = T_1(x)[\gamma]$$

  ισχύει με πιθανότητα $\gamma_{T_1}(\alpha, \gamma)$.



Σχημα 1

- όταν το z επιλέγεται ομοιόμορφα τυχαία μέσα από το $\mathbb{B}^n$, η εξίσωση
$$z[\gamma] = T_2(z)[\beta]$$
ισχύει με πιθανότητα $\gamma_{T_2}(\gamma, \beta)$.
- το ενδεχόμενο $x[\alpha] = T_2\big(T_1(x)\big)[\beta]$ γράφεται και ως

$$\Big(x[\alpha] = T_1(x)[\gamma] \wedge T_1(x)[\gamma] = T_2\big(T_1(x)\big)[\beta]\Big) \\ \vee \Big(x[\alpha] \neq T_1(x)[\gamma] \wedge T_1(x)[\gamma] \neq T_2\big(T_1(x)\big)[\beta]\Big),$$

οπότε η ζητούμενη πιθανότητα είναι η

$$\text{Prob}\Big[x[\alpha] = T_1(x)[\gamma] \wedge T_1(x)[\gamma] = T_2\big(T_1(x)\big)[\beta]\Big] \\ + \text{Prob}\Big[x[\alpha] \neq T_1(x)[\gamma] \wedge T_1(x)[\gamma] \neq T_2\big(T_1(x)\big)[\beta]\Big], \tag{5}$$

για το x διαλεγμένο (και πάλι) ομοιόμορφα τυχαία μέσα από το $\mathbb{B}^n$.
Όμως ο πρώτος όρος της (5) είναι το γινόμενο

$$\text{Prob}\Big[x[\alpha] = T_1(x)[\gamma]\Big] \cdot \text{Prob}\Big[T_1(x)[\gamma] = T_2\big(T_1(x)\big)[\beta] \;\Big|\; x[\alpha] = T_1(x)[\gamma]\Big] \\ = \gamma_{T_1}(\alpha, \gamma) \cdot \theta.$$

Και ο δεύτερος όρος είναι ο

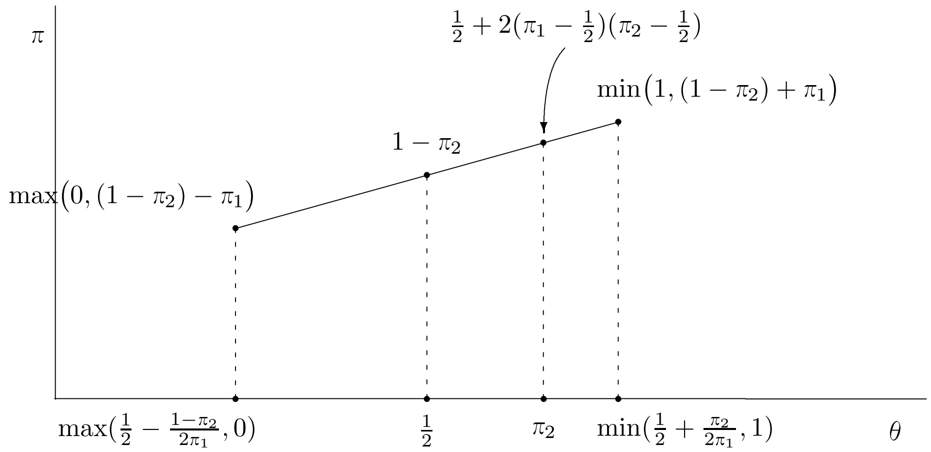
$$1 - \text{Prob}\Big[x[\alpha] = T_1(x)[\gamma] \vee T_1(x)[\gamma] = T_2\big(T_1(x)\big)[\beta]\Big]$$

ή

$$1 - \text{Prob}\Big[x[\alpha] = T_1(x)[\gamma]\Big] - \text{Prob}\Big[T_1(x)[\gamma] = T_2\big(T_1(x)\big)[\beta]\Big] \\ + \text{Prob}\Big[x[\alpha] = T_1(x)[\gamma] \wedge T_1(x)[\gamma] = T_2\big(T_1(x)\big)[\beta]\Big].$$

Όμως ο δεύτερος όρος αυτού του τελευταίου αθροίσματος είναι προφανώς η τιμή $\gamma_{T_1}(\alpha, \gamma)$. Και ο τελευταίος είναι —όπως και πιο πάνω— η τιμή $\gamma_{T_1}(\alpha, \gamma) \cdot \theta$. Εξάλλου, όταν το x κινείται ομοιόμορφα τυχαία στο $\mathbb{B}^n$, το $T_1(x)$ κινείται (βεβαίως όχι ανεξάρτητα προς το x, αλλά ωστόσο) επίσης ομοιόμορφα τυχαία στο $\mathbb{B}^n$, γιατί ο τελεστής T_1 είναι μια μετάθεση· άρα ο τρίτος όρος του αθροίσματος είναι η πιθανότητα

$$\text{Prob}\Big[z[\gamma] = T_2(z)[\beta]\Big],$$



Σχημα 2. Ο τρόπος με τον οποίο μεταβάλλεται η πιθανότητα $\pi = \gamma_T(\alpha,\beta)$ συναρτήσει της θ, με τις $\pi_1 = \gamma_{T_1}(\alpha,\gamma)$ και $\pi_2 = \gamma_{T_2}(\gamma,\beta)$ ως παραμέτρους. Η υπόθεση ότι $\theta = \pi_2$ φαίνεται για την περίπτωση που $\pi_2 > \frac{1}{2}$. Από το σχήμα, η συγκεκριμένη τιμή δεν φαίνεται να επιλέγει κάποιο ιδιαίτερο σημείο πάνω στην καμπύλη της μεταβολής της π ως προς τη θ. Ούτε φαίνεται να εκτιμά την πραγματική τιμή του θ καλύτερα από οποιαδήποτε άλλη τιμή. Είναι απλώς μια από τις επιτρεπτές τιμές της θ.

όταν το z επιλέγεται ομοιόμορφα τυχαία μέσα από στο $\mathbb{B}^n$, και ισούται επομένως με την τιμή $\gamma_{T_2}(\gamma,\beta)$. Τελικά, ο δεύτερος όρος της (5) είναι το άθροισμα

$$1 - \gamma_{T_1}(\alpha,\gamma) - \gamma_{T_2}(\gamma,\beta) + \gamma_{T_1}(\alpha,\gamma)\cdot\theta.$$

Και η πιθανότητα $\gamma_T(\alpha,\beta)$ είναι αυτή που ισχυρίζεται η εκφώνηση. $\dashv$

Στις πρακτικές περιπτώσεις, η Πρόταση 3.5 είναι δύσκολο να χρησιμοποιηθεί για τον υπολογισμό της γραμμικής συμπεριφοράς της σύνθεσης δύο τελεστών από τη γραμμική συμπεριφορά των τελεστών. Η αιτία γι' αυτό είναι η δυσκολία να υπολογίσουμε την πιθανότητα θ. Για να ξεπεράσουμε το σκόπελο, υποθέτουμε αυθαίρετα ότι $\theta = \gamma_{T_2}(\gamma,\beta)$. Αυτό ισοδυναμεί (όπως εύκολα μπορεί κανείς να επιβεβαιώσει) με την υπόθεση ότι η είσοδος στον τελεστή T_2 δεν εξαρτάται από την έξοδο του τελεστή T_1. (Δηλαδή ότι οι τυχαίες μεταβλητές που περιγράφουν τις εισόδους στους δύο τελεστές είναι στοχαστικά ανεξάρτητες.) Αυτό βέβαια είναι λάθος, όπως εξηγείται και στο Σχήμα 2. Παρόλ' αυτά, με τη συγκεκριμένη υπόθεση, ο υπολογισμός της γραμμικής συμπεριφοράς της σύνθεσης γίνεται πολύ απλούστερος.

3.6. Πορισμα. *Στην ειδική περίπτωση που $\theta = \gamma_{T_2}(\gamma,\beta)$ στην Πρόταση 3.5, η γραμμική συμπεριφορά της σύνθεσης T δίνεται από τον τύπο*

$$\gamma_T(\alpha,\beta) = \tfrac{1}{2} + 2\bigl(\gamma_{T_1}(\alpha,\gamma) - \tfrac{1}{2}\bigr)\bigl(\gamma_{T_2}(\gamma,\beta) - \tfrac{1}{2}\bigr).$$

3.7. Πορισμα. *Η αποτελεσματικότητα της σύνθεσης T της προηγούμενης πρότασης είναι η συνάρτηση $\epsilon : \mathbb{B}^n \times \mathbb{B}^n \to [0, \frac{1}{2}]$ που για κάθε δύο μάσκες α, β στο $\mathbb{B}^n$ επιστρέφει την τιμή*

$$\epsilon_T(\alpha,\beta) = \bigl|2\gamma_{T_1}(\alpha,\gamma)\bigl(\theta - \tfrac{1}{2}\bigr) - \bigl(\gamma_{T_2}(\gamma,\beta) - \tfrac{1}{2}\bigr)\bigr|.$$

Και πάλι, γ είναι μια οποιαδήποτε μάσκα στο $\mathbb{B}^n$ και τότε το θ δίνεται από την (4).

Στην ειδική περίπτωση που $\theta = \gamma_{T_2}(\gamma, \beta)$,

$$\epsilon_T(\alpha, \beta) = 2\epsilon_T(\alpha, \gamma)\epsilon_T(\gamma, \beta).$$

Τώρα είναι μια εύκολη επαγωγή να γενικεύσουμε το παραπάνω αποτέλεσμα για την περίπτωση που συνθέτουμε περισσότερους από έναν τελεστές.

3.8. Πρόταση. *Ας είναι $T_1, \ldots, T_\lambda$ τυχούσες μεταθέσεις του $\mathbb{B}^n$ και $T = T_\lambda \circ T_{\lambda-1} \circ \cdots \circ T_1$ η σύνθεσή τους. Η γραμμική συμπεριφορά της T είναι η συνάρτηση $\gamma_T : \mathbb{B}^n \times \mathbb{B}^n \to [0,1]$ που για κάθε δύο μάσκες α και β στο $\mathbb{B}^n$ επιστρέφει την τιμή*

$$\gamma_T(\alpha, \beta) = \sum_{i=1}^{\lambda-1} (-1)^{i+1} 2\gamma_{T_i}(\gamma_{i-1}, \gamma_i)\big(\theta_i - \tfrac{1}{2}\big) + \begin{cases} \gamma_{T_\lambda}(\gamma_{\lambda-1}, \gamma_\lambda) & \text{αν } \lambda = \text{περιττό} \\ 1 - \gamma_{T_\lambda}(\gamma_{\lambda-1}, \gamma_\lambda) & \text{αν } \lambda = \text{άρτιο.} \end{cases}$$

Με γ_0 και γ_λ ονομάσαμε τα α και β αντίστοιχα. Τα $\gamma_1, \ldots, \gamma_{\lambda-1}$ μπορούν να είναι οποιεσδήποτε μάσκες μέσα από το $\mathbb{B}^n$ και τότε

$$\theta_i = \mathrm{Prob}\Big[T_i(x)[\gamma_i] = (T_\lambda \circ \cdots \circ T_{i+1})(x)[\beta] \;\Big|\; x[\gamma_{i-1}] = T_i(x)[\gamma_i]\Big],$$

για κάθε $i = 1, \ldots, \lambda - 1$.

Στην ειδική περίπτωση που $\theta_i = \gamma_{T_\lambda \circ \cdots \circ T_{i+1}}(\gamma_i, \beta)$, ο τύπος της γραμμικής συμπεριφοράς της σύνθεσης είναι ο

$$\gamma_T(\alpha, \beta) = \tfrac{1}{2} + 2^{\lambda-1} \prod_{i=1}^{\lambda} \big(\gamma_{T_i}(\gamma_{i-1}, \gamma_i) - \tfrac{1}{2}\big)$$

Απόδειξη. Με επαγωγή στο πλήθος λ των τελεστών και επαναληπτική χρήση της Πρότασης 3.5 και του Πορίσματος 3.6. ⊣

3.9. Πόρισμα. *Η αποτελεσματικότητα της σύνθεσης T της προηγούμενης πρότασης είναι η συνάρτηση $\epsilon : \mathbb{B}^n \times \mathbb{B}^n \to [0, \frac{1}{2}]$ που για κάθε δύο μάσκες α, β στο $\mathbb{B}^n$ επιστρέφει την τιμή*

$$\epsilon(\alpha, \beta) = \Big|\sum_{i=1}^{\lambda-1} (-1)^{i+1} 2\gamma_{T_i}(\gamma_{i-1}, \gamma_i)\big(\theta_i - \tfrac{1}{2}\big) + (-1)^{\lambda+1}\big(\gamma_{T_\lambda}(\gamma_{\lambda-1}, \gamma_\lambda) - \tfrac{1}{2}\big)\Big|.$$

Τα $\gamma_0, \ldots, \gamma_\lambda$ και $\theta_1, \ldots, \theta_{\lambda-1}$ όπως και πριν.

Στην ειδική περίπτωση που $\theta_i = \gamma_{T_\lambda \circ \cdots \circ T_{i+1}}(\gamma_i, \beta)$, ο τύπος της αποτελεσματικότητας της σύνθεσης είναι ο

$$\epsilon_T(\alpha, \beta) = 2^{\lambda-1} \prod_{i=1}^{\lambda} \epsilon_{T_i}(\gamma_{i-1}, \gamma_i).$$

4. Γραμμική συμπεριφορά του DES

Τώρα θα προσπαθήσουμε να υπολογίσουμε τη γραμμική συμπεριφορά της συνάρτησης κρυπτογράφησης e_k του DES.

Το πρώτο που χρησιμοποιούμε είναι η γραμμική συμπεριφορά των συναρτήσεων αντικατάστασης, από όπου θα μπορέσουμε να υπολογίσουμε μερικώς την αποτελεσματικότητα καθενός από τους γύρους της συνάρτησης κρυπτογράφησης. Στη συνέχεια, χρησιμοποιώντας τα αποτελέσματα της προηγούμενης ενότητας για τη σύνθεση, θα μπορέσουμε να υπολογίσουμε (πάλι μερικώς) την αποτελεσματικότητα όλης της e_k. Το επόμενο λήμμα και τα πορίσματά του εξηγούν τι ακριβώς εννοούμε.

4.1. Λημμα. *Έστω $p, q \in \mathbb{B}^{64}$ η είσοδος και η έξοδος αντίστοιχα του i-οστού γύρου της συνάρτησης κρυπτογράφησης e_k του DES, για κάποιο κλειδί $k \in \mathbb{B}^{56}$. Αν το p διαλέγεται ομοιόμορφα τυχαία, τότε για κάθε $j \in \{1, \dots, 8\}$, κάθε $\alpha \in \mathbb{B}^6$ και κάθε $\beta \in \mathbb{B}^4$, η εξίσωση*[1]

$$(6)\quad p\big[\varepsilon_P\big(\beta \lll_{32} (32-4j)\big) \lll_{64} 32 + \alpha \lll_{32} (31-4j)\big] \\ \oplus q\big[\varepsilon_P\big(\beta \lll_{32} (32-4j)\big)\big] = k\big[\varepsilon_{R_i}^{-1}\big(\alpha \lll_{48} (48-6j)\big)\big]$$

ισχύει με πιθανότητα

$$\gamma_{\alpha_{S'_j}}(\alpha, \beta).$$

Αποδειξη. Έστω ότι το p διαλέγεται ομοιόμορφα τυχαία στο $\mathbb{B}^{64}$. Τότε το $(p^R)_{\langle j\rangle}$ διαλέγεται επίσης ομοιόμορφα τυχαία, στο $\mathbb{B}^6$. Άρα το ίδιο ισχύει και για την ποσότητα

$$B_{(j)} = (p^R)_{\langle j\rangle} \oplus \varepsilon_{R_i}(k)_{(j)},$$

που είναι ακριβώς η είσοδος στην συνάρτηση $\alpha_{S'_j} = \alpha_{S_j} \circ \varepsilon_Z$. Επομένως, η εξίσωση

$$(7)\qquad B_{(j)}[\alpha] = \alpha_{S'_j}(B_{(j)})[\beta]$$

ισχύει με πιθανότητα $\gamma_{\alpha_{S'_j}}(\alpha, \beta)$. Αλλά αυτή η εξίσωση είναι ακριβώς η (6).

Πράγματι, εύκολα υπολογίζουμε ότι

$$\begin{aligned}
B_{(j)}[\alpha] &= \big((p^R)_{\langle j\rangle} \oplus \varepsilon_{R_i}(k)_{(j)}\big)[\alpha] = (p^R)_{\langle j\rangle}[\alpha] \oplus \varepsilon_{R_i}(k)_{(j)}[\alpha],\\
(p^R)_{\langle j\rangle}[\alpha] &= \varepsilon_E(p^R)_{(j)}[\alpha] = p^R[\alpha \lll_{32} (31-4j)] = p[\alpha \lll_{32} (31-4j)],\\
\varepsilon_{R_i}(k)_{(j)}[\alpha] &= \varepsilon_{R_i}(k)[\alpha \lll_{48} (48-6j)] = k\big[\varepsilon_{R_i}^{-1}\big(\alpha \lll_{48} (48-6j)\big)\big],\\
\alpha_{S'_j}(B_{(j)})[\beta] &= C_{(j)}[\beta] = \varepsilon_P^{-1}(D)_{(j)}[\beta] = \varepsilon_P^{-1}(D)[\beta \lll_{32} (32-4j)]\\
&= D\big[\varepsilon_P\big(\beta \lll_{32} (32-4j)\big)\big] = (p^L \oplus q^R)\big[\varepsilon_P\big(\beta \lll_{32} (32-4j)\big)\big]\\
&= p^L\big[\varepsilon_P\big(\beta \lll_{32} (32-4j)\big)\big] \oplus q^R\big[\varepsilon_P\big(\beta \lll_{32} (32-4j)\big)\big]\\
&= p\big[\varepsilon_P\big(\beta \lll_{32} (32-4j)\big) \lll_{64} 32\big] \oplus q\big[\varepsilon_P\big(\beta \lll_{32} (32-4j)\big)\big].
\end{aligned}$$

Τελικά, η (7) γράφεται ως

$$p[\alpha \lll_{32} (31-4j)] \oplus k\big[\varepsilon_{R_i}^{-1}\big(\alpha \lll_{48} (48-6j)\big)\big] \\ = p\big[\varepsilon_P\big(\beta \lll_{32} (32-4j)\big) \lll_{64} 32\big] \oplus q\big[\varepsilon_P\big(\beta \lll_{32} (32-4j)\big)\big],$$

από την οποία άμεσα προκύπτει η (6). ⊣

4.2. Πορισμα. *Για κάθε $i = 1, \dots, 16$, ας είναι f_i ο i-οστός γύρος της συνάρτησης κρυπτογράφησης e_k του DES, για κάποιο $k \in \mathbb{B}^{56}$. Επίσης, για κάθε $j \in \{1, \dots, 8\}$, κάθε $\alpha \in \mathbb{B}^6$ και κάθε $\beta \in \mathbb{B}^4$, ας είναι*

$$\begin{aligned}
A(j, \alpha, \beta) &= \varepsilon_P\big(\beta \lll_{32} (32-4j)\big) \lll_{64} 32 + \alpha \lll_{32} (31-4j),\\
B(j, \alpha, \beta) &= \varepsilon_P\big(\beta \lll_{32} (32-4j)\big),\\
\Gamma(j, \alpha, \beta) &= \varepsilon_{R_i}^{-1}\big(\alpha \lll_{48} (48-6j)\big).
\end{aligned}$$

[1] Χρησιμοποιούμε το συμβολισμό $\varepsilon_{R_i}^{-1}$ εννοώντας τη συνάρτηση που, δεδομένης μιας 48-ψήφιας ακολουθίας y επιστρέφει την 56-ψήφια ακολουθία x που έχει όσο το δυνατόν περισσότερα μηδενικά και επιπλέον ικανοποιεί την $\varepsilon_{R_i}(x) = y$. (Τι είναι;)

Τότε, για όλα τα νόμιμα i, j, α, β, είναι

$$\gamma_{f_i}\big(A(j,\alpha,\beta), B(j,\alpha,\beta)\big) = \begin{cases} \gamma_{\alpha_{S'_j}}(\alpha,\beta) & \text{αν } k\big[\Gamma(j,\alpha,\beta)\big] = 0 \\ 1 - \gamma_{\alpha_{S'_j}}(\alpha,\beta) & \text{αν } k\big[\Gamma(j,\alpha,\beta)\big] = 1. \end{cases}$$

4.3. Πόρισμα. *Για όλα τα νόμιμα (όπως στο Πόρισμα 4.2) i, j, α, β, είναι*

$$\epsilon_{f_i}\big(A(j,\alpha,\beta), B(j,\alpha,\beta)\big) = \epsilon_{\alpha_{S'_j}}(\alpha,\beta).$$

Δηλαδή, τα Πορίσματα 4.2 και 4.3 μας λένε πώς να υπολογίσουμε (το πολύ) $8 \times 2^6 \times 2^4 = 2^{13}$ από τις συνολικά $2^{64} \times 2^{64} = 2^{128}$ διαφορετικές τιμές της γραμμικής συμπεριφοράς και της αποτελεσματικότητας του τυχόντος γύρου της συνάρτησης κρυπτογράφησης του DES.

Από αυτές τις τιμές μπορούμε, σύμφωνα με την Πρόταση 3.8, να υπολογίσουμε ορισμένες τιμές της γραμμικής συμπεριφοράς όλης της συνάρτησης κρυπτογράφησης, ως σύνθεσης των γύρων της: Για κάθε $i = 1, \dots, 16$ διαλέγουμε μια νόμιμη (όπως στο Πόρισμα 4.2) τριάδα (j_i, α_i, β_i), κι έτσι καθορίζουμε μια τριάδα 64-ψήφιων μασκών

$$\begin{aligned} A_i &= A(j_i, \alpha_i, \beta_i), \\ B_i &= B(j_i, \alpha_i, \beta_i), \\ \Gamma_i &= \Gamma(j_i, \alpha_i, \beta_i). \end{aligned}$$

Αν οι επιλογές μας είναι τέτοιες ώστε να ισχύει $B_i = A_{i+1}$, για κάθε $i = 1, \dots, 15$, τότε η ακολουθία μασκών

$$\gamma_0 = A_1,\ \gamma_1 = B_1 = A_2,\ \gamma_2 = B_2 = A_3,\ \dots,\ \gamma_{15} = B_{15} = A_{16},\ \gamma_{16} = B_{16}$$

είναι για τους τελεστές $T_1 = f_1, \dots, T_{16} = f_{16}$ η ακολουθία που περιγράφει η Πρόταση 3.8. Επομένως, μας επιτρέπει να υπολογίσουμε την τιμή της γραμμικής συμπεριφοράς της σύνθεσης $f_{16} \circ \cdots \circ f_1 = e_k$ για το ζευγάρι μασκών (γ_0, γ_{16}), αρκεί να ξέρουμε τις πιθανότητες

$$\gamma_{f_1}(\gamma_0, \gamma_1), \dots, \gamma_{f_{16}}(\gamma_{15}, \gamma_{16}), \qquad \text{και} \qquad \theta_1, \dots, \theta_{15},$$

με τις θ_i όπως ορίζονται στην Πρόταση 3.8.

Αλλά οι θ_i δεν είναι γνωστές και είναι μάλλον πολύ δύσκολο να υπολογιστούν. Για το λόγο αυτό τις παρακάμπτουμε, υποθέτοντας (αυθαίρετα, όπως εξηγήσαμε πιο πάνω) ότι βρισκόμαστε στην ειδική περίπτωση της Πρότασης 3.8.

Οι υπόλοιπες πιθανότητες $\gamma_{f_1}(\gamma_0, \gamma_1), \dots$ είναι γνωστές, από την επιλογή των $\gamma_0, \dots, \gamma_{16}$ και το Πόρισμα 4.2, αρκεί να ξέρουμε τα ψηφία

$$k[\Gamma_1], k[\Gamma_2], \dots, k[\Gamma_{16}].$$

Τότε θα ξέρουμε, από την Πρόταση 3.8, ότι

$$\gamma_{e_k}(\gamma_0, \gamma_{16}) = \tfrac{1}{2} + 2^{15} \prod_{i=1}^{16} \big(\gamma_{f_i}(\gamma_{i-1}, \gamma_i) - \tfrac{1}{2}\big),$$

και άρα, από το Πόρισμα 4.2, ότι

$$\gamma_{e_k}(\gamma_0, \gamma_{16}) = \tfrac{1}{2} + (-1)^{\rho} 2^{15} \prod_{i=1}^{16} \big|\gamma_{f_i}(\gamma_{i-1}, \gamma_i) - \tfrac{1}{2}\big|,$$

όπου

$$\rho = k[\Gamma_1] \oplus \cdots \oplus k[\Gamma_{16}] = k[\Gamma_1 \oplus \cdots \oplus \Gamma_{16}]. \tag{8}$$

Δηλαδή,

$$\gamma_{e_k}(\gamma_0,\gamma_{16}) = \tfrac{1}{2} + (-1)^{\rho} 2^{15} \prod_{i=1}^{16} \epsilon_{f_i}(\gamma_{i-1},\gamma_i), \tag{9}$$

όπου ϵ_{f_i} η αποτελεσματικότητα του i-οστού γύρου, που είναι γνωστή για κάθε $i = 1,\ldots,16$ (Πόρισμα 4.3). Βεβαίως, το ψηφίο ρ δεν είναι γνωστό, κι έτσι η Εξίσωση (9) μπορεί να μας δώσει μόνο την απόσταση της γραμμικής συμπεριφοράς από το $\frac{1}{2}$, και όχι την ακριβή τιμή της. Ισοδύναμα, είναι γνωστή μόνο η αποτελεσματικότητα της συνάρτησης κρυπτογράφησης,

$$\epsilon_{e_k}(\gamma_0,\gamma_{16}) = 2^{15} \prod_{i=1}^{16} \epsilon_{f_i}(\gamma_{i-1},\gamma_i). \tag{10}$$

Και είναι, τέλος, χρήσιμο να σημειώσουμε τις επόμενες προφανείς συνεπαγωγές:

$$\begin{aligned} \rho = 0 &\Longrightarrow \gamma_{e_k}(\gamma_0,\gamma_{16}) \geq \tfrac{1}{2}, \\ \rho = 1 &\Longrightarrow \gamma_{e_k}(\gamma_0,\gamma_{16}) \leq \tfrac{1}{2}. \end{aligned} \tag{11}$$

5. Η τεχνική (συνέχεια)

Τώρα επιστρέφουμε στο σημείο που σταματήσαμε στο τέλος της Ενότητας 2: αναζητάμε μια γραμμική προσέγγιση του DES με όσο το δυνατόν μεγαλύτερη αποτελεσματικότητα. Δηλαδή ψάχνουμε μάσκες $\alpha,\beta \in \mathbb{B}^{64}$ και $\gamma \in \mathbb{B}^{56}$ ώστε, όταν το p κινείται ομοιόμορφα τυχαία στο $\mathbb{B}^{64}$, η Εξίσωση (1) να ισχύει με πιθανότητα π όσο το δυνατόν πιο απομακρυσμένη από το $\frac{1}{2}$.

Ας υποθέσουμε ότι έχουμε κάνει όλη τη διαδικασία της προηγούμενης ενότητας και έχουμε καταλήξει σε μία τιμή $\epsilon = \epsilon_{e_k}(\gamma_0,\gamma_{16})$. Τότε, από τον ορισμό της συνάρτησης ϵ_{e_k}, ξέρουμε ακριβώς ότι είναι ϵ η αποτελεσματικότητα της εξίσωσης

$$p[\gamma_0] = e_k(p)[\gamma_{16}], \qquad \text{ή, ισοδύναμα, της} \quad p[\gamma_0] = q[\gamma_{16}].$$

Αλλά αυτή η εξίσωση γράφεται και ως

$$p[\gamma_0] \oplus q[\gamma_{16}] = 0. \tag{12}$$

Και ξέρουμε ότι τότε είναι επίσης ϵ η αποτελεσματικότητα της εξίσωσης που λέει το ακριβώς ανάποδο, δηλαδή της εξίσωσης

$$p[\gamma_0] \oplus q[\gamma_{16}] = 1. \tag{13}$$

Ακριβέστερα, αυτό που ξέρουμε είναι ότι η μία από τις (12) και (13) ισχύει με πιθανότητα $\frac{1}{2} + \epsilon \geq \frac{1}{2}$, ενώ η άλλη ισχύει με πιθανότητα $\frac{1}{2} - \epsilon \leq \frac{1}{2}$. Αν μάλιστα λάβουμε υπόψη μας την Εξίσωση (11), τότε η εξίσωση που ισχύει με πιθανότητα μεγαλύτερη από το $\frac{1}{2}$ είναι ακριβώς η

$$p[\gamma_0] \oplus q[\gamma_{16}] = \rho,$$

δηλαδή η

$$p[\gamma_0] \oplus q[\gamma_{16}] = k[\Gamma_1 \oplus \cdots \oplus \Gamma_{16}]. \tag{14}$$

Και έτσι η (14) είναι μια εξίσωση στην οποία μπορούμε να εφαρμόσουμε τον Αλγόριθμο 3.

Αυτό λοιπόν που απομένει είναι να ψάξουμε μέσα σε όλες τις γνωστές τιμές της αποτελεσματικότητας της συνάρτησης κρυπτογράφησης του DES, για να βρούμε τη μεγαλύτερη δυνατή. Αυτό γίνεται εξαντλητικά, αλλά βεβαίως μόνο για τις το πολύ 2^{13} γνωστές τιμές της αποτελεσματικότητας.

ΚΕΦΑΛΑΙΟ 6

Advanced Encryption Standard

Παρόλο που έχουν προσφέρει πολλά στην προσπάθεια να κατανοήσουμε και να περιγράψουμε πόσο ισχυρό είναι τελικά το DES, οι κρυπταναλυτικές επιθέσεις των Κεφαλαίων 4 και 5 δεν φαίνεται να αποτελούν τελικά και πάρα πολύ μεγάλη απειλή για όποιους το χρησιμοποιούν για να επικοινωνήσουν. Η αιτία είναι ότι και οι δύο επιθέσεις προϋποθέτουν ότι ξέρουμε πάρα πολλά γνωστά (ή, ακόμη χειρότερα, επιλεγμένα) κείμενα, κάτι που στην πράξη είναι τις πιο πολλές φορές δύσκολο να γίνει.

Πολύ μεγαλύτερη έχει αποδειχθεί η απειλή από το σχετικά μικρό μήκος του κλειδιού. Αυτό οδήγησε πολλούς και από πολύ νωρίς να σκέφτονται σοβαρά την περίπτωση της τετριμμένης επίθεσης που βασίζεται στην εξαντλητική αναζήτηση (Ενότητα 3-4.4) —παρόλο που αυτό είναι περίπου ισοδύναμο με το να ψάχνει κανείς ψύλλο στ' άχυρα, όταν τα άχυρα φτιάχνουν μια στοίβα με βάση 470 στρέμματα και ύψος 150 μέτρα![1]

Ήδη από το 1977 άρχισαν να εμφανίζονται εκτιμήσεις για το κόστος που θα είχε μια μηχανή ειδικά κατασκευασμένη για να βρίσκει κλειδιά του DES με αυτή τη μέθοδο. Σύμφωνα με τους τότε υπολογισμούς [**34**, σελ. 82] μια μηχανή αυτού του είδους θα κόστιζε 20 εκατομμύρια δολάρια και θα μπορούσε να ψάχνει όλο το χώρο των 2^{56} κλειδιών μέσα σε μια μέρα. Αν οι συγκεκριμένοι υπολογισμοί ήταν σωστοί, το μόνο που έλειπε πλέον ήταν η απόφαση κάποιου να κάνει την παραπάνω επένδυση με σκοπό να βρίσκει και να πουλάει κλειδιά του DES. Και ήταν θέμα μιας διαίρεσης για να υπολογίσει πόσο πρέπει να πουλάει το κάθε κλειδί ώστε να αποσβέσει την επένδυσή του μέσα στο επιθυμητό χρονικό διάστημα.

Το 1980 ο Hellman [**11**] παρουσίασε μια μέθοδο αναζήτησης του κλειδιού που μεταφέρει ένα μέρος του κόστους 2^{56} από το χρόνο στο χώρο και είναι επιτυχής με ικανοποιητικά μεγάλη πιθανότητα. Υπολόγισε μάλιστα ότι μια μηχανή που θα εφαρμόζει τη μέθοδό του μπορούσε να κατασκευαστεί με περίπου 4 εκατομμύρια δολάρια και τότε να βρίσκει 100 κλειδιά τη μέρα, με μόνο μια μέρα καθυστέρηση για την εύρεση κάθε κλειδιού. Αν λοιπόν κατασκεύαζε κάποιος αυτή τη μηχανή, τότε, με την υπόθεση ότι η πελατεία θα ήταν αρκετή για να κάνει τη μηχανή να δουλεύει συνέχεια, η απόσβεση της αρχικής του επένδυσης θα μπορούσε να γίνει μέσα σε πέντε χρόνια και με τιμή πώλησης τα μόλις 25 δολάρια για το κάθε κλειδί.

Μετά το 1980, παρόμοιες εκτιμήσεις βασισμένες στην εξαντλητική αναζήτηση εμφανίστηκαν κι άλλες, με όλο και μικρότερο κόστος για τη μηχανή και όλο και μικρότερη καθυστέρηση για την εύρεση ενός κλειδιού. Το 1993, ο Wiener υπολόγισε το κόστος σε 1 εκατομμύριο δολάρια, αν θέλουμε κάθε κλειδί να εντοπίζεται κατά μέσο όρο σε 3.5 ώρες· ή σε μόνο 100 χιλιάδες δολάρια, αν μπορούμε να περιμένουμε μιάμιση μέρα για κάθε εντοπισμό [**34**, σελ. 82].

[1] Υποθέτουμε ότι ο ψύλλος έχει όγκο 1 κυβικό εκατοστό και ότι η στοίβα είναι παραβολοειδής.

Τελικά, η απειλή από την εξαντλητική αναζήτηση αποδείχθηκε και στην πράξη. Το 1997 και με αυτόν ακριβώς το σκοπό, η εταιρεία RSA Data Security, Inc., ανακοίνωσε τη διοργάνωση μια σειρά διαγωνισμών, που ονομάστηκαν DES Challenges, και είχαν αντικείμενο (ουσιαστικά) την εύρεση DES κλειδιών με γνωστά κείμενα.

Ο πρώτος από τους διαγωνισμούς (DES Challenge-I) προκηρύχθηκε τον Ιανουάριο του 1997 με έπαθλο για το νικητή 10 χιλιάδες δολάρια. Μια ομάδα υπό την καθοδήγηση του προγραμματιστή Rocke Verser ετοίμασε το απαραίτητο λογισμικό και οργάνωσε χιλιάδες χρήστες του Διαδικτύου, ώστε καθένας από αυτούς να ψάχνει στον υπολογιστή του ένα διαφορετικό τμήμα του χώρου όλων των κλειδιών. Η αναζήτηση άρχισε το Μάρτιο του ίδιου χρόνου, με ρυθμό που έφθασε μέχρι και τα 7 δισεκατομμύρια κλειδιά το δευτερόλεπτο. Τελικά, και αφού είχε δοκιμαστεί το 25% του συνόλου όλων των κλειδιών, το σωστό κλειδί βρέθηκε τον Ιούνιο, 96 μέρες μετά την έναρξη της αναζήτησης.

Ο δεύτερος από τους διαγωνισμούς (DES Challenge II-1) ξεκίνησε στις 13 Ιανουαρίου του 1998 με έπαθλο από 0 μέχρι και 10 χιλιάδες δολάρια, ανάλογα με το πόσο πιο γρήγορα από τον προηγούμενο διαγωνισμό θα εντοπίζονταν το κλειδί. Ο νικητής ήταν και πάλι μια ομάδα προγραμματιστών, με το όνομα distributed.net, που διασύνδεσε 22 χιλιάδες χρήστες του Διαδικτύου και συνολικά 50 χιλιάδες επεξεργαστές, με αποτέλεσμα να δοκιμάζει μέχρι και 26 τρισεκατομμύρια κλειδιά το δευτερόλεπτο. Τελικά το κλειδί βρέθηκε μετά από 39 μέρες, σε λιγότερο από το μισό του χρόνου που χρησιμοποίησε ο νικητής του προηγούμενου διαγωνισμού και παρόλο που αυτή τη φορά χρειάστηκε να ελεγχθεί υπερτριπλάσιο κομμάτι (85%) του χώρου όλων των κλειδιών.

Τον Ιούλιο του 1998 προκηρύχθηκε και τρίτος διαγωνισμός (DES Challenge II-2). Για πρώτη φορά ο νικητής ήταν μόνο μία μηχανή, σαν αυτές που μέχρι τότε πολλοί είχαν περιγράψει αλλά κανένας δεν κατασκεύαζε (δημόσια τουλάχιστον), ο Deep Crack. Οι συζητήσεις για το σχεδιασμό της είχαν αρχίσει ήδη από το 1997 ανάμεσα στον Paul Kocher της Cryptography Research, Inc., και τον John Gilmore της Electronic Frontier Foundation, και κατέληξαν στην κατασκευή της μετά από ένα περίπου χρόνο και με λιγότερα από 250 χιλιάδες δολάρια. Η μηχανή μπόρεσε να βρει το κλειδί του διαγωνισμού σε μόλις 56 ώρες, έχοντας ψάξει το 25% του χώρου των κλειδιών με το ρυθμό των 92 δισεκατομμυρίων κλειδιών το δευτερόλεπτο.

Στο τέταρτο διαγωνισμό (DES Challenge III), τον Ιανουάριο του 1999, ο Deep Crack συνεργάστηκε με 100 χιλιάδες υπολογιστές της distributed.net, κι έτσι το σωστό κλειδί εντοπίστηκε σε μόλις 22 ώρες και 15 λεπτά.

Ήταν πλέον προφανές ότι το DES δεν αντέχει την τετριμμένη επίθεση, ακριβώς λόγω του μικρού μήκους του κλειδιού. Όμως οι συζητήσεις για την αντικατάσταση του DES είχαν αρχίσει πολύ νωρίτερα, ήδη από το 1993, οπότε και επανεπικυρώθηκε ως πρότυπο για τρίτη συνεχή φορά μετά το 1977. Τότε είχε προταθεί να αντικατασταθεί προσωρινά από το Triple-DES,[2] μέχρις ότου οριστεί κάποιο νέο πρότυπο.

Η συζήτηση για αυτό το νέο πρότυπο άρχισε τον Ιανουάριο του 1997 από το National Institute of Standards and Technology (NIST) του αμερικανικού Υπουργείου Εμπορίου, τον διάδοχο του National Bureau of Standards (NBS) του ίδιου υπουργείου, που είχει ορίσει το DES το 1977. Η διαφορά στη διαδικασία ήταν από την αρχή

[2] Αντί για ένα DES κλειδί, χρησιμοποιούμε τρία και κρυπτογραφούμε το κάθε πακέτο τρεις φορές, μία με κάθε κλειδί· η αποκρυπτογράφηση γίνεται με τρεις απλές αποκρυπτογραφήσεις και τα κλειδιά με την αντίστροφη σειρά. Με αυτό τον τρόπο το μήκος του κλειδιού τριπλασιάζεται και ο χώρος αναζήτησής του γίνεται απαγορευτικά μεγάλος. Όμως υποτριπλασιάζεται η ταχύτητα κρυπτογράφησης και αποκρυπτογράφησης.

	Χώρα	Κρυπτοσύστημα	Σχεδιαστής
	Αυστραλία	LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
(∗)	Βέλγιο	RIJNDAEL	John Daemen, Vincent Rijmen
	Καναδάς	CAST-256	Entrust Technologies, Inc.
	Καναδάς	DEAL	Richard Outerbridge, Lars Knudsen
	Κόστα Ρίκα	FROG	TecApro International S.A.
	Γαλλία	DFC	Centre National pour la Recherche Scientifique (CNRS)
	Γερμανία	MAGENTA	Deutsche Telekom AG
	Ιαπωνία	E2	Nippon Telegraph and Telephone Corporation (NTT)
	Κορέα	CRYPTON	Future Systems, Inc.
	ΗΠΑ	HPC	Rich Schroeppel
(∗)	ΗΠΑ	MARS	IBM
(∗)	ΗΠΑ	RC6	RSA Laboratories
	ΗΠΑ	SAFER+	Cylink Corporation
(∗)	ΗΠΑ	TWOFISH	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson
(∗)	Μ. Βρετανία, Ισραήλ, Νορβηγία	SERPENT	Ross Anderson, Eli Biham, Lars Knudsen

Πινακας 1. Οι 15 υποψηφιότητες για το AES. Με (∗) αυτές που προκρίθηκαν στο δεύτερο γύρο.

προφανής: το νέο πρότυπο θα διαλέγονταν μετά από έναν ανοιχτό και δημόσιο διαγωνισμό, ώστε να μην υπάρξουν ξανά υποψίες παρόμοιες με αυτές που είχε προκαλέσει η μυστικότητα του σχεδιασμού του DES από το National Security Agency (NSA) και την IBM.

Το Σεπτέμβριο του 1997 προσκλήθηκαν οι υποψηφιότητες για το νέο πρότυπο, που ονομάστηκε Advanced Encryption Standard (AES) και είχε από την αρχή τις εξής βασικές προδιαγραφές:

- να είναι κρυπτοσύστημα πακέτου,
- να υποστηρίζει πακέτα των 128 ψηφίων, και
- να υποστηρίζει κλειδιά των 128, 192 και 256 ψηφίων.

Μέχρι τη λήξη της προθεσμίας, τον Ιούνιο του 1998, ανταποκρίθηκαν στην πρόσκληση 15 υποψηφιότητες, από εταιρείες και φυσικά πρόσωπα από διάφορες χώρες (Πίνακας 1). Στον πρώτο γύρο της διαδικασίας, που κράτησε μέχρι τον Αύγουστο του 1999, διοργανώθηκαν συνέδρια με θέμα τα χαρακτηριστικά των υποψήφιων κρυπτοσυστημάτων. Από τα συμπεράσματα αυτών των συνεδρίων και τη δική του ανάλυση, το NIST επέλεξε τελικά πέντε από τα κρυπτοσυστήματα για το δεύτερο γύρο: τα RC6, Mars, Twofish, Serpent και Rijndael.

Γενικές περιγραφές όλων των παραπάνων κρυπτοσυστημάτων και λεπτομερείς περιγραφές των πέντε που προχώρησαν στο δεύτερο γύρο μπορούν να βρεθούν στα [**30, 29, 37, 32, 1, 6**]. Εδώ θα περιγράψουμε μόνο ένα από συστήματα, το RC6. Φαίνεται να πρόκειται για την καλύτερη από τις προτάσεις, καθώς συνδυάζει πολύ καλά την ασφάλεια όχι μόνο με την ταχύτητα, αλλά και με την απλότητα, την ευελιξία και την καινοτομία.

Η υπεροχή του απέναντι στα υπόλοιπα κρυπτοσυστήματα οφείλεται κατά κύριο λόγο στη χρήση περιστροφών που εξαρτώνται από τα δεδομένα (Ενότητα 1-3.1.1).[3] Πρόκειται για πράξεις που εξασφαλίζουν όλη τη μη γραμμικότητα που είναι απαραίτητη για την ασφάλεια κι έτσι ακυρώνουν την αναγκαιότητα των πινάκων αντικατάστασης (Ενότητα 1-3.1.7), που είναι εξαιρετικά δύσκολο να σχεδιαστούν. Ταυτόχρονα, οι εξαρτώμενες από τα δεδομένα περιστροφές μπορούν να υλοποιηθούν πολύ εύκολα και με πολύ μικρό κόστος σε χρόνο (και μάλιστα σταθερό, ανεξάρτητο από το κάθε φορά ποσό της περιστροφής). Το βασικό τους μειονέκτημα είναι ότι, καθώς πρωτοχρησιμοποιήθηκαν πολύ πρόσφατα [**28**], δεν έχουν τύχει ακόμη της εξαντλητικής επίθεσης που θα εδραίωνε στην κρυπτογραφική κοινότητα την σιγουριά για την ασφάλεια που προσφέρουν.

Τέλος, το κρυπτοσύστημα RC6 είναι πλήρως παραμετρικό ως προς το μέγεθος των πακέτων, το μήκος του κλειδιού και το πλήθος των γύρων (που επηρεάζει άμεσα την ταχύτητα και την ασφάλεια), ώστε να μπορεί να χρησιμοποιηθεί σε μια πολύ μεγάλη ποικιλία εφαρμογών.

1. Το κρυπτοσύστημα RC6

Το RC6 είναι μια τριάδα κρυπτοσυστημάτων, όλα μέλη κάποιας παραμετρικής οικογένειας κρυπτοσυστημάτων πακέτου, που την ονομάζουμε RC6-$w/r/b$. Τα w, r και b είναι ακριβώς οι παράμετροι της οικογένειας· αποδίδοντάς τους νόμιμες τιμές ορίζουμε πλήρως και ένα μέλος της. Με τον όρο RC6 αναφερόμαστε στην τριάδα των μελών που ορίζουν οι τιμές $w = 32$, $r = 20$ και $b \in \{16, 24, 32\}$.

Εξηγούμε αμέσως την σημασία των παραμέτρων.

- w: Είναι το μήκος της μικρότερης δυαδικής ακολουθίας στην οποία εκτελεί πράξεις το κρυπτοσύστημα και πρέπει $w = 8d$, για κάποιο $d \geq 1$. Η ιδέα είναι ότι το w θα πρέπει να είναι ίσο με το πλήθος των δυαδικών ψηφίων ανά λέξη στη μηχανή που υλοποιεί το κρυπτοσύστημα, ώστε η κρυπτογράφηση και η αποκρυπτογράφηση να εκτελούνται όσο το δυνατόν ταχύτερα. Σε όλες τις πρακτικές περιπτώσεις οι λέξεις αποτελούνται από bytes και τότε το $d = w/8$ είναι το πλήθος των bytes ανά λέξη. Όπως θα φανεί παρακάτω, η παράμετρος w καθορίζει το μέγεθος του πακέτου του κρυπτοσυστήματος, σε $4w$. Για το AES, που ζητάει 128-ψήφια πακέτα, πρέπει να είναι $w = 32$. Οπότε η υλοποίησή του γίνεται αποτελεσματικότερη σε μηχανές με λέξεις των $d = 4$ bytes.
- r: Είναι το πλήθος των γύρων του κρυπτοσυστήματος και πρέπει απλώς $r \geq 0$.
- b: Είναι το μήκος του κλειδιού του κρυπτοσυστήματος, σε bytes, και πρέπει $0 \leq b \leq 255$. Για το AES, που ζητάει κλειδιά με 128, 192 ή 256 ψηφία, πρέπει να είναι $b \in \{16, 24, 32\}$.

Επομένως, το τυχόν μέλος της οικογένειας RC6-$w/r/b$ είναι ένα κρυπτοσύστημα πακέτου με διαστάσεις $4w \times 8b$. Και υπακούει στις προδιαγραφές του AES μόνο αν

[3] Τέτοιες πράξεις χρησιμοποιεί και το Mars, που όμως υστερεί μάλλον προφανώς έναντι του RC6 σε απλότητα και ευελιξία.

$w = 32$ και $b \in \{16, 24, 32\}$ και το πλήθος r των γύρων του είναι τέτοιο που να εξασφαλίζει την ασφάλεια που απαιτείται από το πρότυπο.

Στη συνέχεια περιγράφουμε γενικά ένα οποιοδήποτε μέλος της οικογένειας. Θα αναφερόμαστε σ' αυτό με το όνομα RC6-$w/r/b$.

1.1. Η συνάρτηση F. Βασική για τη συνέχεια είναι η παρακάτω συνάρτηση,[4] όπου με $\times$ συμβολίζουμε τον πολλαπλασιασμό modulo 2^w,

$$F : \mathbb{B}^w \to \mathbb{B}^w, \qquad \text{με} \quad F(x) = \big(x \times (2x+1)\big) \lll \lg w.$$

Το όρισμά της είναι πάντα ένα από τα τέσσερα κομμάτια στα οποία σπάει ένα πακέτο και η τιμή της χρησιμοποιείται ως το δεύτερο όρισμα είτε μιας διάζευξης με κάποιο άλλο κομμάτι είτε μιας περιστροφής κάποιου άλλου κομματιού.

Η δεύτερη αυτή χρήση είναι που επιβάλλει το $\lll \lg w$· εξηγούμε: Αν $x, y \in \mathbb{B}^w$, τότε σε μια πράξη σαν την

$$y \lll F(x)$$

η ακολουθία y περιστρέφεται προς τα αριστερά κατά το ποσό που αναπαριστούν τα $\lg w$ λιγότερο σημαντικά ψηφία της $F(x)$ (βλέπε και Ενότητα 1-3.1.1). Λοιπόν, θέτοντας $F(x) = \big(x \times (2x+1)\big) \lll \lg w$ και όχι απλά $F(x) = x \times (2x+1)$, στην ουσία φέρνουμε τα $\lg w$ πιο σημαντικά ψηφία της ακολουθίας $x \times (2x+1)$ στη θέση των λιγότερο σημαντικών, ώστε τελικά αυτά να καθορίσουν το ποσό της περιστροφής. Έτσι, η περιστροφή γίνεται κατά ένα ποσό που εξαρτάται από όλα τα ψηφία της ακολουθίας x και όχι μόνο από κάποια από αυτά, όπως θα συνέβαινε αν δεν χρησιμοποιούσαμε την περιστροφή κατά $\lg w$, και αυτό τελικά αυξάνει τη δυσκολία εύρεσης χαρακτηριστικών κατά τη διαφορική κρυπτανάλυση.

1.2. Η little-endian σύμβαση. Όταν μια μηχανή έχει λέξεις των d bytes, η αποθήκευση μιας ακολουθίας $b \geq 0$ bytes απαιτεί προφανώς τουλάχιστον $\lceil b/d \rceil$ λέξεις. Και τότε, χαρακτηριστικά του υλικού επιβάλλουν να κάνουμε την αντιγραφή των bytes στις λέξεις ως εξής: Κατ' αρχήν, επιθέτουμε στην αρχική ακολουθία $d\lceil b/d \rceil - b$ μηδενικά bytes ώστε το νέο μήκος της, $d\lceil b/d \rceil$, να είναι πολλαπλάσιο του d. Στη συνέχεια, αντιγράφουμε το πρώτο (αριστερότερο) byte της νέας ακολουθίας στο λιγότερο σημαντικό (δεξιότερο) byte της πρώτης (αριστερότερης) λέξης. Το δεύτερο byte αντιγράφεται στο αμέσως πιο σημαντικό byte της ίδιας λέξης, κ.λπ., μέχρι που το d-οστό byte να αντιγραφεί στο σημαντικότερο byte της πρώτης λέξης. Στη συνέχεια κάνουμε το ίδιο με τα επόμενα d bytes και τη δεύτερη λέξη, κ.ο.κ., μέχρις ότου εξαντλήσουμε την ακολουθία.

Στο επίπεδο των ακολουθιών δυαδικών ψηφίων, η παραπάνω διαδικασία περιγράφει τη σύνθεση $\varepsilon_{\mathrm{LE}_{d,b}} \circ \mathrm{app}_{d,b}$, όπου

$$\mathrm{app}_{d,b} : \mathbb{B}^{8b} \to \mathbb{B}^{8d\lceil b/d \rceil}, \qquad \text{με} \quad \mathrm{app}_{d,b}(x) = x \,\|\, 00\cdots 0,$$

και $8(d\lceil b/d \rceil - b)$ μηδενικά, ενώ $\mathrm{LE}_{d,b}$ είναι το διάνυσμα του Πίνακα 2. Είναι εύκολο να διαπιστώσει κανείς ότι $\varepsilon_{\mathrm{LE}_{d,b}}^{-1} = \varepsilon_{\mathrm{LE}_{d,b}}$.

[4]Παρά το ίδιο όνομα, η συνάρτηση δεν έχει καμία σχέση με τη συνάρτηση F του DES. Άλλωστε, το RC6-$w/r/b$ δεν έχει τη Feistel δομή —τουλάχιστον όχι έτσι όπως την εξηγήσαμε στην Ενότητα 1-3.2.

$\mathrm{LE}_{d,b}$

$8d-7$	...	...	...	...	...	...	$8d$
...	...	...	...	...	...	...	...
9	10	11	12	13	14	15	16
1	2	3	4	5	6	7	8
$8d+(8d-7)$	...	...	...	...	...	...	$8d+8d$
...	...	...	...	...	...	...	...
$8d+9$	...	...	...	...	...	...	$8d+16$
$8d+1$	...	...	...	...	...	...	$8d+8$
...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...
$(b'-1)8d+(8d-7)$	...	...	...	...	...	...	$(b'-1)8d+8d$
...	...	...	...	...	...	...	...
$(b'-1)8d+9$	...	...	...	...	...	...	$(b'-1)8d+16$
$(b'-1)8d+1$	...	...	...	...	...	...	$(b'-1)8d+8$

Πινακας 2. Το διάνυσμα $\mathrm{LE}_{d,b}$, για την κατά τη little-endian σύμβαση αντιγραφή $d\lceil b/d\rceil$ bytes σε $b' = \lceil b/d\rceil$ λέξεις των d bytes η καθεμιά.

1.3. Τα υποκλειδιά. Καθεμιά από τις συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης χρειάζεται συνολικά $r+2$ υποκλειδιά με $2w$ ψηφία το καθένα, που τα ονομάζουμε σταθερά $u_0, \ldots, u_{r+1}$. Αυτά παράγονται από το βασικό κλειδί σύμφωνα με τη διαδικασία που εξηγούμε παρακάτω.

Κεντρικά αντικείμενα σ' αυτή τη διαδικασία είναι δύο ακολουθίες

$$\alpha = (\alpha_\nu)_{-r' \leq \nu \leq \mu} \qquad \text{και} \qquad \beta = (\beta_\nu)_{-b' \leq \nu \leq \mu},$$

όπου $r' = 2r+4$ είναι το διπλάσιο του πλήθους όλων των υποκλειδιών, $b' = \lceil b/d\rceil$ (όπου $d = \frac{w}{8}$) είναι το μήκος της επέκτασης $\mathrm{app}_{d,b}(k)$ του κλειδιού και $\mu = 3\max(r', b')$ είναι το τριπλάσιο της μεγαλύτερης από αυτές τις σταθερές. (Όμως, στην ειδική περίπτωση που $b = 0$, θέτουμε $b' = 1$.)

Για καθεμιά από τις ακολουθίες, οι όροι της με μη θετικό δείκτη έχουν τιμές που δεν εξαρτώνται από τις τιμές των όρων της άλλης ακολουθίας. Αντίθετα, ένας όρος με θετικό δείκτη εξαρτά την τιμή του από όρους και των δύο ακολουθιών. Θα ορίσουμε πρώτα τα ανεξάρτητα κομμάτια των ακολουθιών και μετά τα αλληλοεξαρτώμενα.

Για το ανεξάτητο κομμάτι της α χρειαζόμαστε δύο «μαγικές» σταθερές, τις P_w και Q_w. Η πρώτη προκύπτει όταν πάρουμε τα πρώτα w ψηφία της δυαδικής αναπαράστασης του κλασματικού μέρους της βάσης του νεπέριου λογαρίθμου και διορθώσουμε την τιμή ώστε να είναι σίγουρα περιττή· για την Q_w χρησιμοποιούμε τη χρυσή τομή. Δηλαδή,

$$P_w = \mathrm{Odd}\big(2^w(e-2)\big) \qquad \text{όπου } e = 2.718281828459\ldots$$
$$Q_w = \mathrm{Odd}\big(2^w(\varphi-2)\big) \qquad \text{όπου } \varphi = 1.618033988749\ldots,$$

με $\mathrm{Odd}(x)$ τη συνάρτηση που στρογγυλεύει το x προς τα πάνω ώστε να γίνει περιττός.

Με δεδομένες τις P_w και Q_w, το ανεξάρτητο κομμάτι της α είναι αυτό που ορίζουν οι εξισώσεις

$$\alpha_{-r'} = P_w$$

$$\alpha_\nu = \alpha_{\nu-1} + Q_w \qquad (-r'+1 \le \nu \le -1)$$
$$\alpha_0 = 0.$$

Δηλαδή πρόκειται για την αριθμητική πρόοδο με βάση P_w και διαφορά Q_w, εκτός από τον τελευταίο όρο, που είναι απλά το μηδέν.

Το ανεξάρτητο κομμάτι της β καθορίζεται από το κλειδί. Απλώς επεκτείνουμε το κλειδί για να αποκτήσει μήκος πολλαπλάσιο του πλήθους d των bytes ανά λέξη και μετά το «αποθηκεύουμε» στην ακολουθία λέξεων

$$\beta_{-b'}, \beta_{-b'+1}, \beta_{-b'+2}, \ldots, \beta_{-1}$$

σύμφωνα με τη little-endian σύμβαση. Το β_0 είναι απλώς μηδέν.

$$\beta_\nu = \big[\varepsilon_{\mathrm{LE}_{d,b}}\big(\mathrm{app}_{d,b}(k)\big)\big]_{v+b'+1,\,w} \qquad (-b' \le \nu \le -1)$$
$$\beta_0 = 0.$$

Τώρα είναι άμεσο να δώσουμε τις εξισώσεις που ορίζουν τους υπόλοιπους όρους των δύο ακολουθιών, αυτούς με θετικό δείκτη:

$$\alpha_\nu = (\alpha_{\nu+1-r'} + \alpha_{\nu-1} + \beta_{\nu-1}) \lll 3 \qquad (1 \le \nu \le \mu)$$
$$\beta_\nu = (\beta_{\nu+1-b'} + \alpha_\nu + \beta_{\nu-1}) \lll (\alpha_\nu + \beta_{\nu-1}) \qquad (1 \le \nu \le \mu).$$

Τελικά, τα υποκλειδιά δίνονται από την εξίσωση

(1) $$u_i = \alpha_{(\mu-r')+(2i+1)} \,\|\, \alpha_{(\mu-r')+(2i+2)} \qquad (0 \le i \le r+1).$$

1.4. Οι συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης. Η κρυπτογράφηση του κάθε $4w$-ψήφιου πακέτου γίνεται με τη διαδοχική εφαρμογή $r+4$ μεταθέσεων. Είναι δηλαδή η συνάρτηση κρυπτογράφησης $e_k : \mathbb{B}^{4w} \to \mathbb{B}^{4w}$ η σύνθεση

$$e_k = \varepsilon_I \circ h_{u_{r+1}} \circ f_{u_r} \circ f_{u_{r-1}} \circ \cdots \circ f_{u_1} \circ g_{u_0} \circ \varepsilon_I.$$

Η πρώτη και η τελευταία από τις μεταθέσεις είναι απλώς οι απαραίτητες για να αντιγραφεί το πακέτο σε 4 λέξεις, ή για να πάρουμε το πακέτο από αυτές τις λέξεις, σύμφωνα με τη litlle-endian σύμβαση. Το διάνυσμα I είναι απλώς το $\mathrm{LE}_{w/8,\,w/2}$. Θυμίζουμε ότι $\varepsilon_I^{-1} = \varepsilon_I$.

Η δεύτερη και η προτελευταία μετάθεση εξασφαλίζουν το απαραίτητη λεύκανση (whitening) που θα κρύψει από τον εχθρό την πρώτη και την τελευταία κρυπτογραφική πράξη. Πρόκειται αντίστοιχα για τις συναρτήσεις

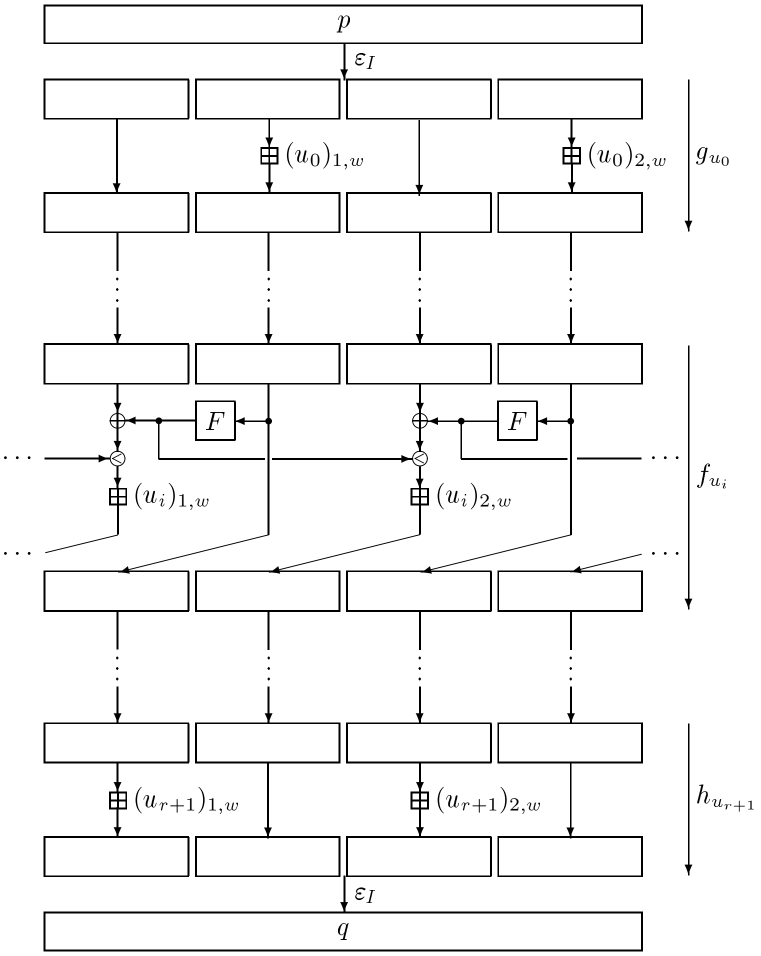
$$g_u : \mathbb{B}^{4w} \to \mathbb{B}^{4w}, \qquad \text{με} \quad g_u(x) = x_{1,w} \,\|(x_{2,w} + u_{1,w}) \,\|\, x_{3,w} \,\|(x_{4,w} + u_{2,w}),$$
$$h_u : \mathbb{B}^{4w} \to \mathbb{B}^{4w}, \qquad \text{με} \quad h_u(x) = (x_{1,w} + u_{1,w}) \,\|\, x_{2,w} \,\|(x_{3,w} + u_{2,w}) \,\|\, x_{4,w},$$

όπου $u \in \mathbb{B}^{2w}$ είναι κάθε φορά το υποκλειδί με το οποίο γίνεται η λεύκανση. Π.χ., η g_u απλά προσθέτει τις δύο λέξεις του υποκλειδιού στη δεύτερη και στην τέταρτη λέξεις της εισόδου. Προφανώς, οι συναρτήσεις αντιστρέφονται από τις

$$g_u^{-1} : \mathbb{B}^{4w} \to \mathbb{B}^{4w}, \qquad \text{με} \quad g_u^{-1}(x) = x_{1,w} \,\|(x_{2,w} - u_{1,w}) \,\|\, x_{3,w} \,\|(x_{4,w} - u_{2,w}),$$
$$h_u^{-1} : \mathbb{B}^{4w} \to \mathbb{B}^{4w}, \qquad \text{με} \quad h_u^{-1}(x) = (x_{1,w} - u_{1,w}) \,\|\, x_{2,w} \,\|(x_{3,w} - u_{2,w}) \,\|\, x_{4,w},$$

Καθεμιά από τις υπόλοιπες r μεταθέσεις είναι, για διαφορετικό κάθε φορά υποκλειδί u, η συνάρτηση $f_u : \mathbb{B}^{4w} \to \mathbb{B}^{4w}$, με

$$f_u(x) = x_{2,w} \,\|\Big(\big[\big(x_{3,w} \oplus F(x_{4,w})\big) \lll F(x_{2,w})\big] + u_{2,w}\Big)$$
$$\|\, x_{4,w} \,\|\Big(\big[\big(x_{1,w} \oplus F(x_{2,w})\big) \lll F(x_{4,w})\big] + u_{1,w}\Big),$$



Σχημα 1. Η συνάρτηση κρυπτογράφησης του RC6-$w/r/b$.

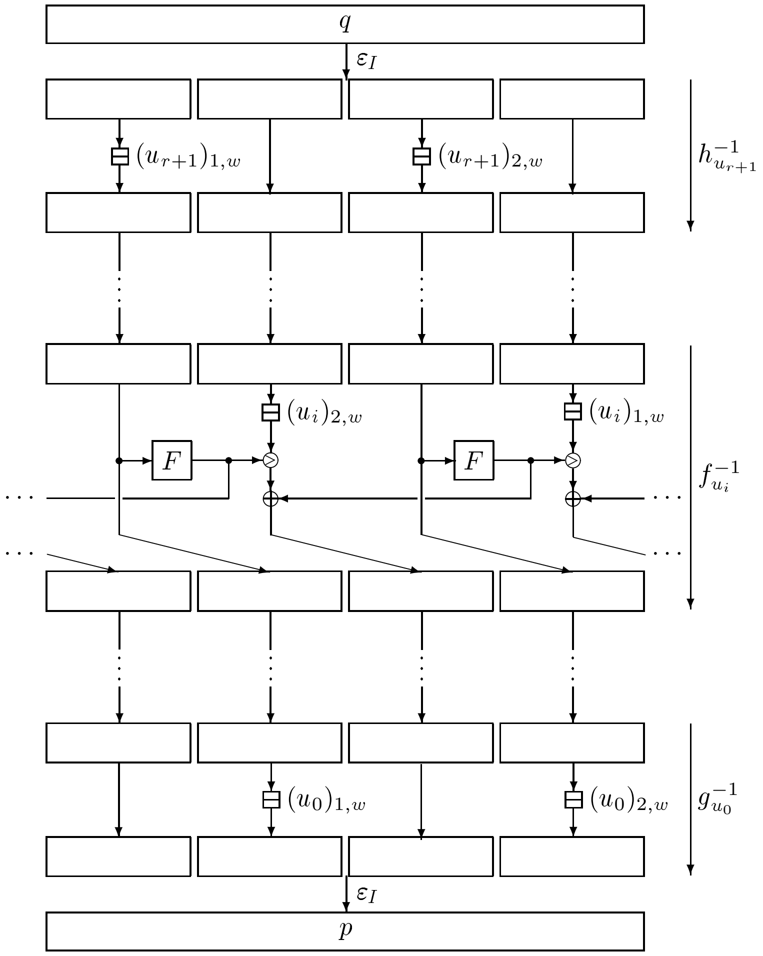
που είναι εύκολο να επιβεβαιώσουμε ότι αντιστρέφεται από την f_u^{-1} με

$$f_u^{-1}(x) = \Big(\Big[(x_{4,w} - u_{1,w}) \ggg F(x_{3,w})\Big] \oplus F(x_{1,w})\Big) \parallel x_{1,w} \\ \parallel \Big(\Big[(x_{2,w} - u_{2,w}) \ggg F(x_{1,w})\Big] \oplus F(x_{3,w})\Big) \parallel x_{3,w}.$$

Οι r μεταθέσεις που ορίζονται με αυτόν τον τρόπο λέμε ότι είναι οι γύροι του κρυπτοσυστήματος. Το Σχήμα 1 εξηγεί καλύτερα τη δομή του κάθε γύρου αλλά και όλης της συνάρτησης κρυπτογράφησης.

Τέλος, η αποκρυπτογράφηση γίνεται απλώς με την αντίστροφη της e_k, δηλαδή τη συνάρτηση

$$\begin{aligned} d_k &= e_k^{-1} \\ &= (\varepsilon_I \circ h_{u_{r+1}} \circ f_{u_r} \circ f_{u_{r-1}} \circ \cdots \circ f_{u_1} \circ g_{u_0} \circ \varepsilon_I)^{-1} \\ &= \varepsilon_I^{-1} \circ g_{u_0}^{-1} \circ f_{u_1}^{-1} \circ f_{u_2}^{-1} \circ \cdots \circ f_{u_r}^{-1} \circ h_{u_{r+1}}^{-1} \circ \varepsilon_I^{-1} \end{aligned}$$



Σχημα 2. Η συνάρτηση αποκρυπτογράφησης του RC6-$w/r/b$.

$$= \varepsilon_I \circ g^{-1}_{u_0} \circ f^{-1}_{u_1} \circ f^{-1}_{u_2} \circ \cdots \circ f^{-1}_{u_r} \circ h^{-1}_{u_{r+1}} \circ \varepsilon_I,$$

που εξηγείται και από το Σχήμα 2.

Παράρτημα

Οι πίνακες κατανομής διαφορών των συναρτήσεων αντικατάστασης του DES

$\alpha_{S_1'}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000001	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
000010	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
000011	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
000100	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
000101	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
000110	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
000111	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
001000	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
001001	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
001010	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
001011	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
001100	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
001101	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
001110	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
001111	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
010000	0	0	0	0	0	0	2	14	0	6	6	12	4	6	8	6
010001	6	8	2	4	6	4	8	6	4	0	6	6	0	4	0	0
010010	0	8	4	2	6	6	4	6	6	4	2	6	6	0	4	0
010011	2	4	4	6	2	0	4	6	2	0	6	8	4	6	4	6
010100	0	8	8	0	10	0	4	2	8	2	2	4	4	8	4	0
010101	0	4	6	4	2	2	4	10	6	2	0	10	0	4	6	4
010110	0	8	10	8	0	2	2	6	10	2	0	2	0	6	2	6
010111	4	4	6	0	10	6	0	2	4	4	4	6	6	6	2	0
011000	0	6	6	0	8	4	2	2	2	4	6	8	6	6	2	2
011001	2	6	2	4	0	8	4	6	10	4	0	4	2	8	4	0
011010	0	6	4	0	4	6	6	6	6	2	2	0	4	4	6	8
011011	4	4	2	4	10	6	6	4	6	2	2	4	2	2	4	2
011100	0	10	10	6	6	0	0	12	6	4	0	0	2	4	4	0
011101	4	2	4	0	8	0	0	2	10	0	2	6	6	6	14	0
011110	0	2	6	0	14	2	0	0	6	4	10	8	2	2	6	2
011111	2	4	10	6	2	2	2	8	6	8	0	0	0	4	6	4
100000	0	0	0	10	0	12	8	2	0	6	4	4	4	2	0	12
100001	0	4	2	4	4	8	10	0	4	4	10	0	4	0	2	8
100010	10	4	6	2	2	8	2	2	2	2	6	0	4	0	4	10
100011	0	4	4	8	0	2	6	0	6	6	2	10	2	4	0	10
100100	12	0	0	2	2	2	2	0	14	14	2	0	2	6	2	4
100101	6	4	4	12	4	4	4	10	2	2	2	0	4	2	2	2
100110	0	0	4	10	10	10	2	4	0	4	6	4	4	4	2	0
100111	10	4	2	0	2	4	2	0	4	8	0	4	8	8	4	4
101000	12	2	2	8	2	6	12	0	0	2	6	0	4	0	6	2
101001	4	2	2	10	0	2	4	0	0	14	10	2	4	6	0	4
101010	4	2	4	6	0	2	8	2	2	14	2	6	2	6	2	2
101011	12	2	2	2	4	6	6	2	0	2	6	2	6	0	8	4
101100	4	2	2	4	0	2	10	4	2	2	4	8	8	4	2	6
101101	6	2	6	2	8	4	4	4	2	4	6	0	8	2	0	6
101110	6	6	2	2	0	2	4	6	4	0	6	2	12	2	6	4
101111	2	2	2	2	2	6	8	8	2	4	4	6	8	2	4	2
110000	0	4	6	0	12	6	2	2	8	2	4	4	6	2	2	4
110001	4	8	2	10	2	2	2	2	6	0	0	2	2	4	10	8
110010	4	2	6	4	4	2	2	4	6	6	4	8	2	2	8	0
110011	4	4	6	2	10	8	4	2	4	0	2	2	4	6	2	4
110100	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6
110101	2	2	4	0	8	0	0	0	14	4	6	8	0	2	14	0
110110	2	6	2	2	8	0	2	2	4	2	6	8	6	4	10	0
110111	2	2	12	4	2	4	4	10	4	4	2	6	0	2	2	4
111000	0	6	2	2	2	0	2	2	4	6	4	4	4	6	10	10
111001	6	2	2	4	12	6	4	8	4	0	2	4	2	4	4	0
111010	6	4	6	4	6	8	0	6	2	2	6	2	2	6	4	0
111011	2	6	4	0	0	2	4	6	4	6	8	6	4	4	6	2
111100	0	10	4	0	12	0	4	2	6	0	4	12	4	4	2	0
111101	0	8	6	2	2	6	0	8	4	4	0	4	0	12	4	4
111110	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
111111	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

ΠΙΝΑΚΑΣ 3. Ο πίνακας κατανομής διαφορών της συνάρτησης $\alpha_{S_1'} = \alpha_{S_1} \circ \varepsilon_Z$.

$\alpha_{S'_2}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000001	0	0	0	4	0	2	6	4	0	14	8	6	8	4	6	2
000010	0	0	0	2	0	4	6	4	0	0	4	6	10	10	12	6
000011	4	8	4	8	4	6	4	2	4	2	2	4	6	2	0	4
000100	0	0	0	0	0	6	0	14	0	6	10	4	10	6	4	4
000101	2	0	4	8	2	4	6	6	2	0	8	4	2	4	10	2
000110	0	12	6	4	6	4	6	2	2	10	2	8	2	0	0	0
000111	4	6	6	4	2	4	4	2	6	4	2	4	4	6	0	6
001000	0	0	0	4	0	4	0	8	0	10	16	6	6	0	6	4
001001	14	2	4	10	2	8	2	6	2	4	0	0	2	2	2	4
001010	0	6	6	2	10	4	10	2	6	2	2	4	2	2	4	2
001011	6	2	2	0	2	4	6	2	10	2	0	6	6	4	4	8
001100	0	0	0	4	0	14	0	10	0	6	2	4	4	8	6	6
001101	6	2	6	2	10	2	0	4	0	10	4	2	8	2	2	4
001110	0	6	12	8	0	4	2	0	8	2	4	4	6	2	0	6
001111	0	8	2	0	6	6	8	2	4	4	4	6	8	0	4	2
010000	0	0	0	8	0	4	10	2	0	2	8	10	0	10	6	4
010001	6	6	4	6	4	0	6	4	8	2	10	2	2	4	0	0
010010	0	6	2	6	2	4	12	4	6	4	0	4	4	6	2	2
010011	4	0	4	0	8	6	6	0	0	2	0	6	4	8	2	14
010100	0	6	6	4	10	0	2	12	6	2	2	2	4	4	2	2
010101	6	8	2	0	8	2	0	2	2	2	2	2	2	14	10	2
010110	0	8	6	4	2	2	4	2	6	4	6	2	6	0	6	6
010111	6	4	8	6	4	4	0	4	6	2	4	4	4	2	4	2
011000	0	6	4	6	10	4	0	2	4	8	0	0	4	8	2	6
011001	2	4	6	4	4	2	4	2	6	4	6	8	0	6	4	2
011010	0	6	8	4	2	4	2	2	8	2	2	6	2	4	4	8
011011	0	6	4	4	0	12	6	4	2	2	2	4	4	2	10	2
011100	0	4	6	6	12	0	4	0	10	2	6	2	0	0	10	2
011101	0	6	2	2	6	0	4	16	4	4	2	0	0	4	6	8
011110	0	4	8	2	10	6	6	0	8	4	0	2	4	4	0	6
011111	4	2	6	6	2	2	2	4	8	6	10	6	4	0	0	2
100000	0	0	0	2	0	12	10	4	0	0	0	2	14	2	8	10
100001	0	4	6	8	2	10	4	2	2	6	4	2	6	2	0	6
100010	4	12	8	4	2	2	0	0	2	8	8	6	0	6	0	2
100011	8	2	0	2	8	4	2	6	4	8	2	2	6	4	2	4
100100	10	4	0	0	0	4	0	2	6	8	6	10	8	0	2	4
100101	6	0	12	2	8	6	10	0	0	8	2	6	0	0	2	2
100110	2	2	4	4	2	2	10	14	2	0	4	2	2	4	6	4
100111	6	0	0	2	6	4	2	4	4	4	8	4	8	0	6	6
101000	8	0	8	2	4	12	2	0	2	6	2	0	6	2	0	10
101001	0	2	4	10	2	8	6	4	0	10	0	2	10	0	2	4
101010	4	0	4	8	6	2	4	4	6	6	2	6	2	2	4	4
101011	2	2	6	4	0	2	2	6	2	8	8	4	4	4	8	2
101100	10	6	8	6	0	6	4	4	4	2	4	4	0	0	2	4
101101	2	2	2	4	0	0	0	2	8	4	4	6	10	2	14	4
101110	2	4	0	2	10	4	2	0	2	2	6	2	8	8	10	2
101111	12	4	6	8	2	6	2	8	0	4	0	2	0	8	2	0
110000	0	4	0	2	4	4	8	6	10	6	2	12	0	0	0	6
110001	0	10	2	0	6	2	10	2	6	0	2	0	6	6	4	8
110010	8	4	6	0	6	4	4	8	4	6	8	0	2	2	2	0
110011	2	2	6	10	2	0	0	6	4	4	12	8	4	2	2	0
110100	0	12	6	4	6	0	4	4	4	0	4	6	4	2	4	4
110101	0	12	4	6	2	4	4	0	10	0	0	8	0	8	0	6
110110	8	2	4	0	4	0	4	2	0	8	4	2	6	16	2	2
110111	6	2	2	2	6	6	4	8	2	2	6	2	2	2	4	8
111000	0	8	8	10	6	2	2	0	4	0	4	2	4	0	4	10
111001	0	2	0	0	8	0	10	4	10	0	8	4	4	4	4	6
111010	4	0	2	8	4	2	2	2	4	8	2	0	4	10	10	2
111011	16	4	4	2	8	2	2	6	4	4	4	2	0	2	2	2
111100	0	2	6	2	8	4	6	0	10	2	2	4	4	10	4	0
111101	0	16	10	2	4	2	4	2	8	0	0	8	0	6	2	0
111110	4	4	0	10	2	4	2	14	4	2	6	6	0	0	6	0
111111	4	0	0	2	0	8	2	4	0	2	4	4	4	14	10	6

ΠΙΝΑΚΑΣ 4. Ο πίνακας κατανομής διαφορών της συνάρτησης $\alpha_{S'_2} = \alpha_{S_2} \circ \varepsilon_Z$.

$\alpha_{S'_3}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000001	0	0	0	2	0	4	2	12	0	14	0	4	8	2	6	10
000010	0	0	0	2	0	2	0	8	0	4	12	10	4	6	8	8
000011	8	6	10	4	8	6	0	6	4	4	0	0	0	4	2	2
000100	0	0	0	4	0	2	4	2	0	12	8	4	6	8	10	4
000101	6	2	4	8	6	10	6	2	2	8	2	0	2	0	4	2
000110	0	10	6	6	10	0	4	12	2	4	0	0	6	4	0	0
000111	2	0	0	4	4	4	4	2	10	4	4	8	4	4	4	6
001000	0	0	0	10	0	4	4	6	0	6	6	6	6	0	8	8
001001	10	2	0	2	10	4	6	2	0	6	0	4	6	2	4	6
001010	0	10	6	0	14	6	4	0	4	6	6	0	4	0	2	2
001011	2	6	2	10	2	2	4	0	4	2	6	0	2	8	14	0
001100	0	0	0	8	0	12	12	4	0	8	0	4	2	10	2	2
001101	8	2	8	0	0	4	2	0	2	8	14	2	6	2	4	2
001110	0	4	4	2	4	2	4	4	10	4	4	4	4	4	2	8
001111	4	6	4	6	2	2	4	8	6	2	6	2	0	6	2	4
010000	0	0	0	4	0	12	4	8	0	4	2	6	2	14	0	8
010001	8	2	2	6	4	0	2	0	8	4	12	2	10	0	2	2
010010	0	2	8	2	4	8	0	8	8	0	2	2	4	2	14	0
010011	4	4	12	0	2	2	2	10	2	2	2	2	4	4	4	8
010100	0	6	4	4	6	4	6	2	8	6	6	2	2	0	0	8
010101	4	8	2	8	2	4	8	0	4	2	2	2	2	6	8	2
010110	0	6	10	2	8	4	2	0	2	2	2	8	4	6	4	4
010111	0	6	6	0	6	2	4	4	6	2	2	10	6	8	2	0
011000	0	8	4	6	6	0	6	2	4	0	4	2	10	0	6	6
011001	4	2	4	8	4	2	10	2	2	2	6	8	2	6	0	2
011010	0	8	6	4	4	0	6	4	4	8	0	10	2	2	2	4
011011	4	10	2	0	2	4	2	4	8	2	2	8	4	2	8	2
011100	0	6	8	8	4	2	8	0	12	0	10	0	4	0	2	0
011101	0	2	0	6	2	8	4	6	2	0	4	2	4	10	0	14
011110	0	4	8	2	4	6	0	4	10	0	2	6	4	8	4	2
011111	0	6	8	0	10	6	4	6	4	2	2	10	4	0	0	2
100000	0	0	0	0	0	4	4	8	0	2	2	4	10	16	12	2
100001	10	8	8	0	8	4	2	4	0	6	6	6	0	0	2	0
100010	12	6	4	4	2	4	10	2	0	4	4	2	4	4	0	2
100011	2	2	0	6	0	2	4	0	4	12	4	2	6	4	8	8
100100	4	8	2	12	6	4	2	10	2	2	2	4	2	0	4	0
100101	6	0	2	0	8	2	0	2	8	8	2	2	4	4	10	6
100110	6	2	0	4	4	0	4	0	4	2	14	0	8	10	0	6
100111	0	2	4	16	8	6	6	6	0	2	4	4	0	2	2	2
101000	6	2	10	0	6	4	0	4	4	2	4	8	2	2	8	2
101001	0	2	8	4	0	4	0	6	4	10	4	8	4	4	4	2
101010	2	6	0	4	2	4	4	6	4	8	4	4	4	2	4	6
101011	10	2	6	6	4	4	8	0	4	2	2	0	2	4	4	6
101100	10	4	6	2	4	2	2	2	4	10	4	4	0	2	6	2
101101	4	2	4	4	4	2	4	16	2	0	0	4	4	2	6	6
101110	4	0	2	10	0	6	10	4	2	6	6	2	2	0	2	8
101111	8	2	0	0	4	4	4	2	6	4	6	2	4	8	4	6
110000	0	10	8	6	2	0	4	2	10	4	4	6	2	0	6	0
110001	2	6	2	0	4	2	8	8	2	2	2	0	2	12	6	6
110010	2	0	4	8	2	8	4	4	8	4	2	8	6	2	0	2
110011	4	4	6	8	6	6	0	2	2	2	6	4	12	0	0	2
110100	0	6	2	2	16	2	2	2	12	2	4	0	4	2	0	8
110101	4	6	0	10	8	0	2	2	6	0	0	6	2	10	2	6
110110	4	4	4	4	0	6	6	4	4	4	4	4	0	6	2	8
110111	4	8	2	4	2	2	6	0	2	4	8	4	10	0	6	2
111000	0	8	12	0	2	2	6	6	2	10	2	2	0	8	0	4
111001	2	6	4	0	6	4	6	4	8	0	4	4	2	4	8	2
111010	6	0	2	2	4	6	4	4	4	2	2	6	12	2	6	2
111011	2	2	6	0	0	10	4	8	4	2	4	8	4	4	0	6
111100	0	2	4	2	12	2	0	6	2	0	2	8	4	6	4	10
111101	4	6	8	6	2	2	2	2	10	2	6	6	2	4	2	0
111110	8	6	4	4	2	10	2	0	2	2	4	2	4	2	10	2
111111	2	6	4	0	0	10	8	2	2	8	6	4	6	2	0	4

Πινακας 5. Ο πίνακας κατανομής διαφορών της συνάρτησης $\alpha_{S'_3} = \alpha_{S_3} \circ \varepsilon_Z$.

$\alpha_{S'_4}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000001	0	0	0	0	0	16	16	0	0	16	16	0	0	0	0	0
000010	0	0	0	8	0	4	4	8	0	4	4	8	8	8	8	0
000011	8	6	2	0	2	4	8	2	6	0	4	6	0	6	2	8
000100	0	0	0	8	0	0	12	4	0	12	0	4	8	4	4	8
000101	4	2	2	8	2	12	0	2	2	0	12	2	8	2	2	4
000110	0	8	8	4	8	8	0	0	8	0	8	0	4	0	0	8
000111	4	2	6	4	6	0	16	6	2	0	0	2	4	2	6	4
001000	0	0	0	4	0	8	4	8	0	4	8	8	4	8	8	0
001001	8	4	4	4	4	0	8	4	4	0	0	4	4	4	4	8
001010	0	6	6	0	6	4	4	6	6	4	4	6	0	6	6	0
001011	0	12	0	8	0	0	0	0	12	0	0	12	8	12	0	0
001100	0	0	0	4	0	8	4	8	0	4	8	8	4	8	8	0
001101	8	4	4	4	4	0	0	4	4	8	0	4	4	4	4	8
001110	0	6	6	4	6	0	4	6	6	4	0	6	4	6	6	0
001111	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
010000	0	0	0	0	0	8	12	4	0	12	8	4	0	4	4	8
010001	4	2	2	16	2	4	0	2	2	0	4	2	16	2	2	4
010010	0	0	0	8	0	4	4	8	0	4	4	8	8	8	8	0
010011	8	2	6	0	6	4	0	6	2	8	4	2	0	2	6	8
010100	0	8	8	0	8	0	8	0	8	8	0	0	0	0	0	16
010101	8	4	4	0	4	8	0	4	4	0	8	4	0	4	4	8
010110	0	8	8	4	8	8	0	0	8	0	8	0	4	0	0	8
010111	4	6	2	4	2	0	0	2	6	16	0	6	4	6	2	4
011000	0	8	8	8	8	4	0	0	8	0	4	0	8	0	0	8
011001	4	4	4	0	4	4	16	4	4	0	4	4	0	4	4	4
011010	0	6	6	4	6	0	4	6	6	4	0	6	4	6	6	0
011011	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
011100	0	8	8	8	8	4	0	0	8	0	4	0	8	0	0	8
011101	4	4	4	0	4	4	0	4	4	16	4	4	0	4	4	4
011110	0	6	6	0	6	4	4	6	6	4	4	6	0	6	6	0
011111	0	0	12	8	12	0	0	12	0	0	0	0	8	0	12	0
100000	0	0	0	8	0	0	0	12	0	0	0	12	8	12	12	0
100001	0	4	8	0	8	4	8	8	4	0	4	4	0	4	8	0
100010	8	2	2	0	2	4	8	6	2	8	4	6	0	6	6	0
100011	4	6	2	8	2	4	0	2	6	0	4	6	8	6	2	4
100100	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
100101	0	8	4	4	4	0	0	4	8	8	0	8	4	8	4	0
100110	0	6	6	0	6	4	8	2	6	8	4	2	0	2	2	8
100111	4	6	2	8	2	4	0	2	6	0	4	6	8	6	2	4
101000	16	4	4	0	4	4	4	4	4	4	4	4	0	4	4	0
101001	0	6	2	8	2	4	0	2	6	8	4	6	8	6	2	0
101010	0	2	2	16	2	4	4	2	2	4	4	2	16	2	2	0
101011	8	0	4	0	4	8	16	4	0	0	8	0	0	0	4	8
101100	8	4	4	4	4	0	8	4	4	8	0	4	4	4	4	0
101101	4	2	6	4	6	8	0	6	2	0	8	2	4	2	6	4
101110	16	0	0	0	0	16	0	0	0	0	16	0	0	0	0	16
101111	16	0	0	0	0	0	16	0	0	16	0	0	0	0	0	16
110000	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
110001	0	8	4	4	4	0	0	4	8	8	0	8	4	8	4	0
110010	16	6	6	4	6	0	4	2	6	4	0	2	4	2	2	0
110011	0	2	6	4	6	8	8	6	2	0	8	2	4	2	6	0
110100	0	12	12	8	12	0	0	0	12	0	0	0	8	0	0	0
110101	0	4	8	0	8	4	8	8	4	0	4	4	0	4	8	0
110110	0	2	2	4	2	0	4	6	2	4	0	6	4	6	6	16
110111	0	2	6	4	6	8	8	6	2	0	8	2	4	2	6	0
111000	0	4	4	0	4	4	4	4	4	4	4	4	0	4	4	16
111001	0	6	2	8	2	4	0	2	6	8	4	6	8	6	2	0
111010	0	4	4	0	4	8	8	4	4	8	8	4	0	4	4	0
111011	16	4	4	0	4	0	0	4	4	0	0	4	0	4	4	16
111100	0	4	4	4	4	0	8	4	4	8	0	4	4	4	4	8
111101	4	2	6	4	6	8	0	6	2	0	8	2	4	2	6	4
111110	0	2	2	8	2	12	4	2	2	4	12	2	8	2	2	0
111111	8	4	0	8	0	0	0	0	4	16	0	4	8	4	0	8

ΠΙΝΑΚΑΣ 6. Ο πίνακας κατανομής διαφορών της συνάρτησης $\alpha_{S'_4} = \alpha_{S_4} \circ \varepsilon_Z$.

$\alpha_{S_5'}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000001	0	0	0	4	0	10	8	6	0	4	2	2	12	10	2	4
000010	0	0	0	4	0	10	6	4	0	6	4	2	4	8	10	6
000011	8	2	4	6	4	4	2	2	6	8	6	4	4	0	2	2
000100	0	0	0	8	0	4	10	6	0	6	6	4	8	6	0	6
000101	12	2	0	4	0	4	8	2	4	0	16	2	0	2	0	8
000110	0	8	4	6	4	6	2	2	4	4	6	0	6	0	2	10
000111	2	0	4	8	4	2	6	6	2	8	6	2	2	0	6	6
001000	0	0	0	2	0	8	10	4	0	4	10	4	8	4	4	6
001001	8	6	0	4	0	6	6	2	2	10	2	8	6	2	0	2
001010	0	6	8	6	0	8	0	0	8	10	4	2	8	0	0	4
001011	4	2	2	4	8	10	6	4	2	6	2	2	6	2	2	2
001100	0	0	0	10	0	2	10	2	0	6	10	6	6	6	2	4
001101	10	4	2	2	0	6	16	0	0	2	10	2	2	4	0	4
001110	0	6	4	8	4	6	10	2	4	4	4	2	4	0	2	4
001111	4	4	0	8	0	2	0	2	8	2	4	2	8	4	4	12
010000	0	0	0	0	0	4	4	12	0	2	8	10	4	6	12	2
010001	6	6	10	10	4	0	2	6	2	4	0	6	2	4	2	0
010010	0	2	4	2	10	4	0	10	8	6	0	6	0	6	6	0
010011	0	0	6	2	8	0	0	4	4	6	2	8	2	8	10	4
010100	0	12	2	6	4	0	4	4	8	4	4	4	6	2	4	0
010101	4	8	0	2	8	0	2	4	2	2	4	2	4	8	8	6
010110	0	6	10	2	14	0	2	2	4	4	0	6	0	4	6	4
010111	0	6	8	4	8	4	0	2	8	4	0	2	2	8	6	2
011000	0	10	8	0	6	4	0	4	4	4	6	4	4	4	0	6
011001	0	4	6	2	4	4	2	6	4	2	2	4	12	2	10	0
011010	0	2	16	2	12	2	0	6	4	0	0	4	0	4	4	8
011011	2	8	12	0	0	2	2	6	8	4	0	6	0	0	8	6
011100	0	10	2	6	6	6	6	4	8	2	0	4	4	4	2	0
011101	4	6	2	0	8	2	4	6	6	0	8	6	2	4	2	4
011110	0	2	6	2	4	0	0	2	12	2	2	6	2	10	10	4
011111	0	6	8	4	8	8	0	6	6	2	0	6	0	6	2	2
100000	0	0	0	8	0	8	2	6	0	4	4	4	6	6	8	8
100001	0	0	0	6	6	2	6	4	6	10	14	4	0	0	4	2
100010	14	4	0	10	0	2	12	2	2	2	10	2	0	0	2	2
100011	2	0	0	4	2	2	10	4	0	8	8	2	6	8	0	8
100100	6	2	8	4	4	4	6	2	2	6	6	2	6	2	2	2
100101	6	0	0	8	2	8	2	6	6	4	2	2	4	2	6	6
100110	12	0	0	4	0	4	4	4	0	8	4	0	12	8	0	4
100111	12	2	0	2	0	12	2	2	4	4	8	4	8	2	2	0
101000	2	8	4	6	2	4	6	0	6	6	4	0	2	2	2	10
101001	6	4	6	8	8	4	6	2	0	0	2	2	10	0	2	4
101010	4	4	0	2	2	4	6	2	0	0	6	4	10	4	4	12
101011	4	6	2	6	0	0	12	2	0	4	12	2	6	4	0	4
101100	8	6	2	6	4	8	6	0	4	4	0	2	6	0	6	2
101101	4	4	0	4	0	6	4	2	4	12	0	4	4	6	4	6
101110	6	0	2	4	0	6	6	4	2	10	6	10	6	2	0	0
101111	10	4	0	2	2	6	10	2	0	2	2	4	6	2	2	10
110000	0	4	8	4	6	4	0	6	10	4	2	4	2	6	4	0
110001	0	6	6	4	10	2	0	0	4	4	0	0	4	6	12	6
110010	4	6	0	2	6	4	6	0	6	0	4	6	4	10	6	0
110011	8	10	0	14	8	0	0	8	2	0	2	4	0	4	4	0
110100	0	4	4	2	14	4	0	8	6	8	2	2	0	4	6	0
110101	0	4	16	0	8	4	0	4	4	4	0	8	0	4	4	4
110110	4	4	4	6	2	2	2	12	2	4	4	8	2	4	4	0
110111	4	2	2	2	4	2	0	8	2	2	2	12	6	2	8	6
111000	0	4	8	4	12	0	0	8	10	2	0	0	0	4	2	10
111001	0	8	12	0	2	2	2	2	12	4	0	8	0	4	4	4
111010	0	14	4	0	4	6	0	0	6	2	10	8	0	0	4	6
111011	0	2	2	2	4	4	8	6	8	2	2	2	6	14	2	0
111100	0	0	10	2	6	0	0	2	6	2	2	10	2	4	10	8
111101	0	6	12	2	4	8	0	8	8	2	2	0	2	2	4	4
111110	4	4	10	0	2	4	8	8	2	2	0	2	6	8	4	0
111111	8	6	6	0	4	2	2	4	4	2	8	6	2	4	6	0

Πινακασ 7. Ο πίνακας κατανομής διαφορών της συνάρτησης $\alpha_{S_5'} = \alpha_{S_5} \circ \varepsilon_Z$.

$\alpha_{S'_6}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000001	0	0	0	6	0	2	6	2	0	4	2	4	6	16	14	2
000010	0	0	0	2	0	10	6	10	0	2	4	8	6	6	8	2
000011	0	8	0	8	0	6	4	6	4	4	4	12	2	4	2	0
000100	0	0	0	8	0	0	8	0	0	6	8	10	2	4	10	8
000101	10	2	4	4	4	8	8	4	2	2	0	4	0	8	0	4
000110	0	8	4	4	8	4	2	2	12	0	2	6	6	2	2	2
000111	6	6	4	0	2	10	2	2	2	2	6	6	8	0	6	2
001000	0	0	0	6	0	2	16	4	0	2	6	2	4	12	6	4
001001	10	4	2	6	0	2	6	2	4	0	8	6	4	4	2	4
001010	0	14	4	4	0	2	2	2	10	4	4	4	6	4	2	2
001011	4	6	2	0	2	2	12	8	2	2	2	6	8	2	0	6
001100	0	0	0	12	0	10	4	6	0	8	4	4	2	12	2	0
001101	12	0	2	10	6	4	4	2	4	2	6	0	2	6	0	4
001110	0	6	4	0	4	4	10	8	6	2	4	6	2	0	6	2
001111	2	2	2	2	6	2	6	2	10	4	8	2	6	4	4	2
010000	0	0	0	8	0	8	0	12	0	4	2	6	8	4	6	6
010001	6	2	6	4	6	2	6	4	6	6	4	2	4	0	6	0
010010	0	8	4	2	0	4	2	0	4	10	6	2	8	6	4	4
010011	6	6	12	0	12	2	0	6	6	2	0	4	0	2	4	2
010100	0	4	6	2	8	6	0	2	6	10	4	0	2	4	6	4
010101	2	2	6	6	4	4	2	6	2	6	8	4	4	0	4	4
010110	0	4	14	6	8	4	2	6	2	0	2	0	4	2	0	10
010111	2	6	8	0	0	2	0	2	2	6	0	8	8	2	12	6
011000	0	4	6	6	8	4	2	2	6	4	6	4	2	4	2	4
011001	2	6	0	2	4	4	4	6	4	8	6	4	2	2	6	4
011010	0	6	6	0	8	2	4	6	4	2	4	6	2	0	4	10
011011	0	4	10	2	4	4	2	6	6	6	2	2	6	6	2	2
011100	0	0	8	2	12	2	6	2	8	6	6	2	4	0	4	2
011101	2	4	0	6	8	6	0	2	6	8	6	0	2	4	0	10
011110	0	10	8	2	8	2	0	2	6	4	2	4	6	4	2	4
011111	0	6	6	8	6	4	2	4	4	2	2	0	2	4	2	12
100000	0	0	0	0	0	6	6	4	0	4	8	8	4	6	10	8
100001	2	8	6	8	4	4	6	6	8	4	0	4	0	2	2	0
100010	16	2	4	6	2	4	2	0	6	4	8	2	0	2	2	4
100011	0	4	0	4	4	6	10	4	2	2	6	2	4	6	6	4
100100	10	8	0	6	12	6	10	4	8	0	0	0	0	0	0	0
100101	0	2	4	2	0	4	4	0	4	0	10	10	4	10	6	4
100110	2	2	0	12	2	2	6	2	4	4	8	0	6	6	8	0
100111	8	4	0	8	2	4	2	4	0	6	2	4	4	8	2	6
101000	6	8	4	6	0	4	2	2	4	8	2	6	4	2	2	4
101001	2	4	4	0	8	8	6	8	6	4	0	4	4	4	2	0
101010	6	0	0	6	6	4	6	8	2	4	0	2	2	4	6	8
101011	12	0	4	0	0	4	2	2	2	6	10	6	10	2	4	0
101100	4	2	6	0	0	6	8	6	4	2	2	8	4	6	4	2
101101	6	2	2	6	6	4	4	2	6	2	4	8	4	2	4	2
101110	4	6	2	4	2	4	4	2	4	2	4	6	4	10	4	2
101111	10	0	4	8	0	6	6	2	0	4	4	2	6	2	2	8
110000	0	12	8	2	0	6	0	0	6	6	0	2	8	2	6	6
110001	2	6	10	4	2	2	2	4	6	0	2	6	0	2	4	12
110010	4	2	2	8	10	8	8	6	0	2	2	4	4	2	2	0
110011	4	2	2	2	6	0	4	0	10	6	6	4	0	4	8	6
110100	0	4	4	2	6	4	0	4	6	2	6	4	2	8	0	12
110101	6	12	4	2	4	2	2	4	8	2	2	0	6	4	4	2
110110	0	2	2	4	4	4	4	0	2	10	12	4	0	10	4	2
110111	10	2	2	6	14	2	2	6	2	0	4	6	2	0	4	2
111000	0	4	14	0	8	2	0	4	4	4	2	0	8	2	4	8
111001	2	4	8	0	6	2	0	6	2	6	4	2	8	6	2	6
111010	8	4	0	4	6	2	0	4	6	8	6	0	6	0	4	6
111011	0	4	6	6	2	2	2	14	0	12	0	4	2	2	8	0
111100	0	6	16	0	2	2	2	8	4	2	0	12	6	2	2	0
111101	0	6	2	2	2	6	8	2	4	2	6	2	6	2	4	10
111110	4	2	2	4	4	0	6	10	4	2	4	6	6	2	6	2
111111	0	4	6	6	4	8	4	0	4	8	4	0	4	8	2	2

ΠΙΝΑΚΑΣ 8. Ο πίνακας κατανομής διαφορών της συνάρτησης $\alpha_{S'_6} = \alpha_{S_6} \circ \varepsilon_Z$.

$\alpha_{S'_7}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000001	0	0	0	2	0	4	4	14	0	12	4	6	2	6	6	4
000010	0	0	0	0	0	12	2	2	0	4	0	4	8	12	6	14
000011	8	2	12	2	6	8	6	0	6	4	4	2	2	0	0	2
000100	0	0	0	8	0	4	4	8	0	8	8	12	2	6	2	2
000101	6	0	0	2	8	0	8	4	0	2	6	0	10	6	6	6
000110	0	2	12	0	8	4	8	2	4	4	4	2	6	0	6	2
000111	4	6	4	12	0	4	2	0	0	14	2	6	4	0	0	6
001000	0	0	0	8	0	0	6	10	0	4	12	4	6	6	0	8
001001	10	8	4	8	6	2	2	0	2	6	8	2	0	6	0	0
001010	0	10	6	2	12	2	4	0	4	4	6	4	4	0	0	6
001011	0	2	2	2	4	8	6	4	4	0	4	2	6	4	2	14
001100	0	0	0	4	0	4	8	4	0	2	6	0	14	12	8	2
001101	6	6	2	4	2	6	4	6	6	4	8	8	0	2	0	0
001110	0	12	10	10	0	2	4	2	8	6	4	2	0	0	2	2
001111	2	0	0	0	6	8	8	0	6	2	4	6	8	0	6	8
010000	0	0	0	4	0	2	8	6	0	6	4	10	8	4	8	4
010001	6	10	10	4	4	2	0	4	4	0	2	8	4	2	2	2
010010	0	0	8	8	2	8	2	8	6	4	2	8	0	0	8	0
010011	4	4	2	2	8	6	0	2	2	2	0	4	6	8	14	0
010100	0	8	6	2	8	8	2	6	4	2	0	2	8	6	0	2
010101	4	4	8	2	4	0	4	10	8	2	4	4	4	2	0	4
010110	0	6	10	2	2	2	2	4	10	8	2	2	0	4	10	0
010111	8	2	4	2	6	4	0	6	4	4	2	2	0	4	8	8
011000	0	16	2	2	6	0	6	0	6	2	8	0	6	0	2	8
011001	0	8	0	2	4	4	10	4	8	0	6	4	2	6	2	4
011010	0	2	4	8	12	4	0	6	4	4	0	2	0	6	4	8
011011	0	6	2	6	4	2	4	4	6	4	8	4	2	0	10	2
011100	0	8	4	4	2	6	6	6	6	4	6	8	0	2	0	2
011101	4	4	4	0	0	2	4	2	4	2	2	4	10	10	8	4
011110	0	0	2	2	12	6	2	0	12	2	2	4	2	6	8	4
011111	2	2	10	14	2	4	2	4	4	6	0	2	4	8	0	0
100000	0	0	0	14	0	8	4	2	0	4	2	8	2	6	0	14
100001	4	2	6	2	12	2	4	0	6	4	10	2	4	2	2	2
100010	10	6	0	2	4	4	10	0	4	0	12	2	8	0	0	2
100011	0	6	2	2	2	4	6	10	0	4	8	2	2	6	0	10
100100	4	2	0	6	8	2	6	0	8	2	2	0	8	2	12	2
100101	2	0	2	16	2	4	6	4	6	8	2	4	0	6	0	2
100110	6	10	0	10	0	6	4	4	2	2	4	6	2	4	2	2
100111	4	0	2	0	2	2	14	0	4	6	6	2	12	2	4	4
101000	14	4	6	4	4	6	2	0	6	6	2	2	4	0	2	2
101001	2	2	0	2	0	8	4	2	4	6	4	4	6	4	12	4
101010	2	4	0	0	0	2	8	12	0	8	2	4	8	4	4	6
101011	16	6	2	4	6	10	2	2	2	2	2	2	4	2	2	0
101100	2	6	6	8	2	2	0	6	0	8	4	2	2	6	8	2
101101	6	2	4	2	8	8	2	8	2	4	4	0	2	0	8	4
101110	2	4	8	0	2	2	2	4	0	2	8	4	14	6	0	6
101111	2	2	2	8	0	2	2	6	4	6	8	8	6	2	0	6
110000	0	6	8	2	8	4	4	0	10	4	4	6	0	0	2	6
110001	0	8	4	0	6	2	2	6	6	0	0	2	6	4	8	10
110010	2	4	0	0	6	4	10	6	6	4	6	2	4	6	2	2
110011	0	16	6	8	2	0	2	2	4	2	8	4	0	4	6	0
110100	0	4	14	8	2	2	2	4	16	2	2	2	0	2	0	4
110101	0	6	0	0	10	8	2	2	6	0	0	8	6	4	4	8
110110	2	0	2	2	4	6	4	4	2	2	4	2	4	16	10	0
110111	6	6	6	8	4	2	4	4	4	0	6	8	2	4	0	0
111000	0	2	2	2	8	8	0	2	2	2	0	6	6	4	10	10
111001	4	4	16	8	0	6	4	2	4	4	2	6	0	2	2	0
111010	16	6	4	0	2	0	2	6	0	4	8	10	0	0	4	2
111011	2	0	0	2	0	4	4	4	2	6	2	6	6	12	12	2
111100	0	0	8	0	12	8	2	6	6	4	0	2	2	4	6	4
111101	2	4	12	2	2	2	0	4	6	10	2	6	4	2	0	6
111110	4	6	6	6	2	0	4	8	2	10	4	6	0	4	2	0
111111	14	0	0	0	8	0	6	8	4	2	0	0	4	8	4	6

ΠΙΝΑΚΑΣ 9. Ο πίνακας κατανομής διαφορών της συνάρτησης $\alpha_{S'_7} = \alpha_{S_7} \circ \varepsilon_Z$.

$\alpha_{S_8'}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000001	0	0	0	6	0	16	10	0	0	0	6	0	14	6	2	4
000010	0	0	0	8	0	10	4	2	0	10	2	4	8	8	6	2
000011	6	0	2	8	2	6	4	0	6	6	6	2	2	0	8	6
000100	0	0	0	2	0	4	6	12	0	6	8	4	10	4	8	0
000101	4	10	6	0	0	2	6	0	4	10	4	6	8	2	0	2
000110	0	0	10	4	6	4	4	8	2	6	4	2	4	2	2	6
000111	6	2	8	2	8	10	6	6	4	2	0	4	0	0	0	6
001000	0	0	0	4	0	6	4	2	0	8	6	10	8	2	2	12
001001	8	4	0	6	0	4	4	6	2	4	6	2	12	2	0	4
001010	0	0	16	4	6	6	4	0	4	6	4	2	2	0	0	10
001011	2	8	0	6	2	6	0	4	4	10	0	2	10	2	6	2
001100	0	0	0	2	0	10	10	6	0	6	6	6	2	6	10	0
001101	6	0	4	10	2	0	8	6	2	2	6	10	2	2	2	2
001110	0	0	6	8	4	8	0	2	10	6	2	4	6	2	4	2
001111	8	0	4	2	2	4	2	2	2	6	4	6	0	2	14	6
010000	0	0	0	4	0	0	8	12	0	0	8	8	2	10	6	6
010001	0	6	4	6	2	2	6	6	4	6	4	6	0	4	4	4
010010	0	4	0	8	6	2	8	4	2	4	4	6	2	4	10	0
010011	4	2	2	6	8	6	2	2	14	2	2	4	2	2	2	4
010100	0	16	4	2	6	0	2	6	4	0	4	6	4	6	4	0
010101	0	10	6	0	6	0	2	8	2	2	0	8	2	6	6	6
010110	0	12	6	4	6	0	0	0	8	6	6	2	2	6	4	2
010111	0	6	8	0	6	2	4	6	6	0	2	6	4	4	2	8
011000	0	12	2	2	8	0	8	0	10	4	4	2	4	2	0	6
011001	6	4	8	0	8	0	4	2	0	0	12	2	4	6	2	6
011010	0	4	6	2	8	8	0	4	8	0	0	0	6	2	0	16
011011	2	4	8	10	2	4	2	8	2	4	8	2	0	2	4	2
011100	0	12	6	4	6	4	2	2	6	0	4	4	2	10	2	0
011101	8	6	0	0	10	0	0	8	10	4	2	2	2	8	4	0
011110	0	4	8	6	8	2	4	4	10	2	2	4	2	0	6	2
011111	4	2	4	2	6	2	4	0	2	6	2	2	2	16	8	2
100000	0	0	0	16	0	4	0	0	0	14	6	4	2	0	4	14
100001	0	0	2	10	2	8	10	0	0	6	6	0	10	2	2	6
100010	8	0	6	0	6	4	10	2	0	6	8	0	4	4	2	4
100011	4	8	0	6	0	4	8	6	2	2	10	4	8	0	0	2
100100	4	0	4	8	4	6	2	4	8	6	2	0	0	4	4	8
100101	0	4	6	8	2	8	8	0	4	2	4	4	2	2	6	4
100110	2	6	0	6	4	4	4	6	6	0	4	4	10	4	2	2
100111	6	6	0	0	2	2	6	2	4	4	6	10	2	6	2	6
101000	10	2	6	2	4	12	12	0	2	2	4	0	0	0	2	6
101001	4	0	0	14	2	10	4	2	8	6	4	0	4	2	2	2
101010	8	8	0	2	0	2	4	0	2	6	8	14	2	8	0	0
101011	2	2	0	0	4	2	10	4	6	2	4	0	6	4	8	10
101100	2	6	6	2	4	6	2	0	2	6	4	0	6	4	10	4
101101	8	0	4	4	6	2	0	0	6	8	2	4	6	4	4	6
101110	6	2	2	4	2	2	6	12	4	0	4	2	8	8	0	2
101111	8	12	4	6	6	4	2	2	2	2	4	2	2	4	0	4
110000	0	4	6	2	10	2	2	2	4	8	0	0	8	4	6	6
110001	4	6	8	0	4	6	0	4	4	6	10	2	2	4	4	0
110010	6	6	6	2	4	6	0	2	0	6	8	2	2	6	6	2
110011	6	6	4	2	4	0	0	10	2	2	0	6	8	4	0	10
110100	0	2	12	4	10	4	0	4	12	0	2	4	2	2	2	4
110101	6	4	4	0	10	0	0	4	10	0	0	4	2	8	8	4
110110	4	6	2	2	2	2	6	8	6	4	2	6	0	4	10	0
110111	2	2	8	2	4	4	4	2	6	2	0	10	6	10	2	0
111000	0	4	8	4	2	6	6	2	4	2	2	4	6	4	4	6
111001	4	4	4	8	0	6	0	6	4	8	2	2	2	4	8	2
111010	8	8	0	4	2	0	10	4	0	0	0	4	8	6	8	2
111011	8	2	6	4	4	4	4	0	6	4	4	6	4	4	4	0
111100	0	6	6	6	6	0	0	8	8	2	4	8	4	2	4	0
111101	2	2	8	0	10	0	2	12	0	4	0	8	0	2	6	8
111110	6	4	0	0	4	4	0	10	6	2	6	12	2	4	0	4
111111	0	6	6	0	4	4	6	10	0	6	8	2	0	4	8	0

ΠΙΝΑΚΑΣ 10. Ο πίνακας κατανομής διαφορών της συνάρτησης $\alpha_{S_8'} = \alpha_{S_8} \circ \varepsilon_Z$.

Οι πίνακες διατήρησης ισοτιμιών των συναρτήσεων αντικατάστασης του **DES**

$\alpha_{S_1'}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000010	32	30	30	28	30	32	28	38	34	32	32	38	36	30	26	36
000011	32	30	30	28	30	32	28	38	34	40	32	30	36	38	26	28
000100	32	34	30	28	30	32	28	26	30	36	40	34	32	30	26	44
000101	32	30	30	32	30	28	28	30	34	28	28	34	36	22	30	28
000110	32	32	32	36	32	36	32	32	32	28	36	36	32	32	28	24
000111	32	28	32	40	32	32	32	36	36	28	24	28	36	32	32	32
001000	32	36	30	38	26	26	32	28	28	28	34	30	34	30	32	32
001001	32	32	38	26	30	26	36	28	32	28	30	38	34	26	32	28
001010	32	30	32	34	32	38	40	34	30	32	30	36	30	32	30	36
001011	32	34	24	30	28	22	36	34	26	40	34	36	30	28	30	32
001100	32	30	32	38	32	34	32	34	34	32	38	28	34	28	38	32
001101	32	38	32	38	36	30	28	30	34	32	38	36	30	40	26	28
001110	32	32	30	30	34	34	32	32	36	36	38	30	34	34	28	36
001111	32	32	30	38	30	30	36	28	28	28	30	30	30	30	32	32
010000	32	34	34	32	30	32	36	26	32	38	34	28	38	28	28	14
010001	32	34	30	28	34	28	28	42	28	34	34	28	30	28	32	26
010010	32	36	32	32	28	36	32	36	26	34	34	38	34	38	38	22
010011	32	36	28	28	32	32	24	20	30	30	26	38	34	38	34	34
010100	32	36	32	36	24	28	36	32	34	38	30	34	38	34	30	34
010101	32	32	36	28	28	36	36	28	42	34	34	34	26	34	38	30
010110	32	38	34	32	34	28	32	34	36	34	34	32	30	32	32	34
010111	32	34	38	24	38	36	32	30	20	30	30	32	26	32	32	30
011000	32	34	40	34	32	38	36	34	36	30	36	38	32	30	28	34
011001	32	30	36	26	32	26	32	34	36	26	40	38	32	34	32	26
011010	32	32	26	34	30	30	36	36	30	30	32	32	28	36	34	34
011011	32	36	38	34	22	34	24	36	30	26	36	32	36	32	30	34
011100	32	28	34	34	34	26	32	28	30	30	36	32	32	36	34	34
011101	32	36	30	30	34	26	28	32	34	34	28	32	20	32	26	26
011110	32	34	32	30	36	30	32	30	32	38	28	30	32	30	32	34
011111	32	34	28	34	28	30	36	34	36	26	36	30	28	34	32	34
100000	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100010	32	34	30	32	34	32	32	38	30	32	28	38	36	42	42	32
100011	32	34	30	32	34	32	32	38	38	32	36	22	28	26	34	32
100100	32	34	26	24	34	36	36	34	34	32	32	34	32	38	22	32
100101	32	30	34	36	34	32	28	30	30	32	36	34	28	38	26	32
100110	32	36	36	28	40	24	36	32	32	24	32	28	32	36	32	32
100111	32	32	28	24	24	36	28	28	36	24	28	28	36	36	28	32
101000	32	36	30	30	30	30	28	32	36	36	34	38	30	26	44	36
101001	32	32	30	26	34	30	24	40	32	28	30	30	38	30	28	32
101010	32	34	32	30	32	34	32	30	34	24	26	28	34	32	34	28
101011	32	22	32	34	28	34	36	38	30	32	22	36	34	28	26	32
101100	32	38	28	34	40	34	36	38	30	28	30	44	30	24	30	32
101101	32	30	28	34	28	30	32	34	30	28	30	36	26	36	34	28
101110	32	28	34	38	38	26	24	36	28	32	34	38	38	34	36	32
101111	32	28	34	30	34	22	44	32	28	32	34	30	42	38	32	36
110000	32	30	30	32	30	36	32	34	32	34	38	36	38	32	32	30
110001	32	30	34	36	34	32	32	26	28	30	30	28	30	32	28	34
110010	32	28	28	28	32	32	32	36	30	30	26	30	26	38	34	34
110011	32	28	32	32	36	28	32	28	26	34	34	30	34	30	30	30
110100	32	40	24	40	36	36	32	32	30	30	34	26	38	38	30	30
110101	32	36	28	32	24	28	32	28	30	34	30	34	34	30	30	34
110110	32	38	34	24	34	28	40	34	36	26	34	32	38	32	32	34
110111	32	34	22	32	38	36	40	30	36	38	30	32	34	32	32	30
111000	32	22	36	34	28	30	36	30	36	34	32	38	28	38	28	30
111001	32	34	32	26	28	34	32	30	28	38	28	30	36	34	40	30
111010	32	32	38	30	38	38	32	32	34	34	32	32	40	32	34	34
111011	32	36	34	30	30	42	36	32	18	30	36	32	32	28	30	34
111100	32	32	42	30	26	30	32	40	26	38	32	24	28	36	30	34
111101	32	40	30	34	26	30	36	36	30	26	32	32	32	32	30	34
111110	32	34	32	30	24	34	36	34	32	30	36	30	28	34	36	30
111111	32	18	20	26	32	34	32	30	28	26	44	30	32	30	36	30

ΠΙΝΑΚΑΣ 11. Ο πίνακας διατήρησης ισοτιμιών της συνάρτησης $\alpha_{S_1'} = \alpha_{S_1} \circ \varepsilon_Z$.

$\alpha_{S'_2}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000010	32	32	32	36	32	32	28	32	32	32	28	32	32	32	32	36
000011	32	32	36	24	32	40	32	28	32	32	24	28	32	40	28	40
000100	32	30	34	36	34	32	36	38	32	38	30	32	34	32	32	42
000101	32	34	34	32	34	28	36	26	32	26	38	36	26	36	32	30
000110	32	30	30	28	30	28	32	30	28	34	34	32	34	32	36	42
000111	32	34	34	28	30	32	36	30	28	38	38	32	26	28	32	34
001000	32	32	34	34	30	34	36	32	30	26	28	32	32	32	42	26
001001	32	32	30	30	30	34	40	36	30	34	32	28	32	40	22	30
001010	32	28	34	34	34	34	28	24	34	34	36	32	32	36	26	34
001011	32	36	34	42	34	34	36	32	34	34	36	32	32	28	34	34
001100	32	30	36	30	32	34	32	38	30	32	34	32	34	32	26	28
001101	32	26	32	30	32	38	36	22	38	28	38	32	34	28	30	36
001110	32	26	32	34	32	30	24	38	30	36	34	32	34	36	30	32
001111	32	30	32	30	32	34	32	42	38	40	34	36	34	32	30	36
010000	32	32	28	36	32	32	32	32	32	32	36	36	36	20	28	20
010001	32	32	32	32	32	24	36	36	32	32	40	32	28	36	40	32
010010	32	32	32	36	32	40	32	36	32	32	28	40	28	20	32	44
010011	32	32	24	36	32	40	40	36	32	32	28	32	36	28	40	28
010100	32	30	26	28	30	36	28	30	28	34	34	28	38	28	32	34
010101	32	42	30	28	30	32	32	30	36	38	38	28	30	32	36	34
010110	32	30	26	32	34	32	36	34	40	30	34	32	38	36	32	30
010111	32	42	34	36	34	36	28	30	32	34	34	28	30	32	32	34
011000	32	28	34	30	34	34	36	36	30	30	36	36	32	36	30	34
011001	32	36	26	38	34	34	36	28	30	30	36	28	40	36	30	34
011010	32	40	30	34	30	34	32	32	34	38	32	32	32	32	34	30
011011	32	24	42	38	30	34	36	28	34	30	28	28	24	32	30	26
011100	32	34	40	30	32	30	32	34	34	32	26	36	42	28	34	32
011101	32	30	32	34	32	26	32	30	34	36	34	32	42	32	34	36
011110	32	30	32	38	32	34	36	30	34	36	30	32	34	32	34	32
011111	32	34	28	38	32	30	24	30	18	32	34	32	34	36	30	32
100000	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100010	32	32	32	36	32	24	36	32	32	32	28	16	32	24	24	36
100011	32	32	28	32	32	32	32	36	32	32	32	36	32	32	28	32
100100	32	30	30	32	30	28	36	22	32	38	26	28	38	36	40	34
100101	32	26	30	36	30	32	36	34	32	34	34	24	30	32	40	30
100110	32	38	26	32	18	32	32	30	28	26	30	36	30	28	28	34
100111	32	34	38	32	34	28	28	30	28	38	26	36	38	32	32	26
101000	32	28	34	30	34	34	32	24	34	34	32	40	40	28	26	30
101001	32	28	30	26	34	34	36	28	26	34	28	28	32	28	30	26
101010	32	40	34	30	38	26	32	32	30	34	32	32	32	32	26	30
101011	32	32	26	30	38	42	32	32	22	42	32	32	24	32	34	30
101100	32	26	32	38	32	30	28	30	34	24	34	36	30	32	34	40
101101	32	30	28	30	32	26	32	22	34	36	30	36	22	28	30	32
101110	32	30	28	34	40	34	36	30	26	28	26	36	30	36	30	36
101111	32	26	36	30	24	30	36	34	26	32	42	32	38	32	30	32
110000	32	32	28	36	28	28	36	36	32	32	28	28	32	32	24	32
110001	32	32	32	32	36	28	32	32	32	32	32	24	32	24	28	36
110010	32	32	32	36	36	36	36	32	32	32	36	32	32	32	28	32
110011	32	32	32	28	28	28	28	32	32	32	28	32	32	32	36	32
110100	32	22	30	24	38	36	24	34	36	34	38	24	30	28	36	30
110101	32	26	34	32	30	32	36	34	28	30	26	32	30	32	32	30
110110	32	30	30	36	26	32	40	30	32	38	38	36	30	36	28	34
110111	32	34	30	24	18	36	32	34	40	34	30	32	30	32	28	30
111000	32	32	34	34	26	30	28	32	34	30	32	28	28	28	34	34
111001	32	40	42	26	34	38	36	32	26	22	40	28	36	28	34	34
111010	32	28	30	38	30	30	24	36	30	30	36	32	28	32	30	30
111011	32	28	34	34	22	38	28	32	22	30	32	28	36	32	34	34
111100	32	30	28	30	36	30	32	30	30	32	34	32	34	24	30	32
111101	32	34	36	42	28	42	24	26	38	36	34	28	34	36	30	28
111110	32	34	20	30	36	34	28	34	38	20	30	28	34	36	30	32
111111	32	30	24	30	28	30	32	26	30	32	34	36	34	32	34	32

ΠΙΝΑΚΑΣ 12. Ο πίνακας διατήρησης ισοτιμιών της συνάρτησης $\alpha_{S'_2} = \alpha_{S_2} \circ \varepsilon_Z$.

$\alpha_{S_3'}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000010	32	34	30	28	32	30	26	36	32	38	30	24	36	30	30	28
000011	32	30	30	32	36	30	30	28	28	30	34	32	28	34	30	32
000100	32	28	32	32	34	30	26	34	32	36	36	28	26	22	38	30
000101	32	32	32	28	34	34	34	38	32	32	36	32	34	26	38	34
000110	32	30	34	32	34	28	32	34	32	26	30	32	30	36	40	30
000111	32	30	34	32	30	40	36	38	28	30	34	28	22	36	32	30
001000	32	32	38	26	32	32	34	30	30	34	32	40	38	34	36	28
001001	32	32	34	30	32	24	30	26	30	34	28	28	30	34	40	32
001010	32	30	40	30	32	34	24	26	34	32	38	36	30	32	34	28
001011	32	34	28	38	36	34	32	30	30	32	30	32	30	28	30	36
001100	32	32	30	30	34	42	36	28	34	30	32	28	36	24	38	26
001101	32	28	34	30	34	30	32	44	34	34	36	36	36	36	34	34
001110	32	30	28	30	34	28	30	28	30	36	34	36	36	30	24	30
001111	32	30	24	34	30	32	30	28	26	24	34	36	36	30	36	34
010000	32	32	34	30	34	34	40	36	34	38	28	44	28	24	34	42
010001	32	32	30	34	30	30	32	36	30	34	36	28	36	32	22	38
010010	32	30	36	34	30	32	34	36	30	28	26	32	32	18	36	30
010011	32	34	32	34	30	36	30	20	30	32	30	40	24	30	32	30
010100	32	36	26	30	28	32	34	30	34	26	24	32	38	30	32	32
010101	32	40	30	38	32	40	34	34	30	34	24	28	30	34	36	32
010110	32	34	32	22	32	38	32	34	30	32	34	32	34	32	30	32
010111	32	42	36	26	32	30	28	30	30	32	30	36	34	32	34	28
011000	32	32	36	28	34	34	30	30	28	36	36	36	30	38	38	30
011001	32	40	28	28	30	30	34	34	32	32	32	40	22	30	22	30
011010	32	26	34	32	30	36	28	30	28	34	34	36	38	32	32	30
011011	32	30	34	28	30	32	28	34	36	30	34	32	30	36	32	34
011100	32	32	28	32	28	36	24	36	32	24	36	32	28	36	40	36
011101	32	36	36	36	32	36	28	28	36	40	32	32	36	32	32	40
011110	32	26	38	32	32	30	34	32	24	30	30	28	36	30	30	32
011111	32	26	22	32	32	38	26	32	32	30	30	36	36	30	30	32
100000	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100010	32	30	30	32	32	34	34	24	32	34	30	28	36	34	38	48
100011	32	34	30	28	36	26	38	24	28	34	34	28	28	30	38	28
100100	32	36	32	40	34	30	26	34	36	32	24	40	38	34	34	26
100101	32	32	32	28	34	26	34	30	36	36	40	36	30	30	34	38
100110	32	34	26	20	34	32	32	30	28	26	34	32	34	28	28	30
100111	32	34	26	36	30	28	36	34	40	30	38	28	26	28	36	30
101000	32	32	34	30	32	40	38	34	30	26	28	36	30	42	32	32
101001	32	32	30	34	32	32	34	30	30	26	40	40	38	26	36	36
101010	32	34	36	30	40	30	28	34	34	28	34	28	30	28	30	36
101011	32	30	40	30	28	22	36	30	30	20	26	32	30	32	26	36
101100	32	32	34	26	34	42	32	32	30	34	32	28	32	28	30	34
101101	32	36	38	34	34	38	28	24	30	30	36	28	32	32	26	34
101110	32	34	24	30	26	32	34	28	34	36	34	32	32	30	32	26
101111	32	34	36	34	38	36	34	28	46	24	34	32	32	30	28	30
110000	32	32	26	30	30	30	28	32	34	30	36	36	32	36	30	38
110001	32	32	30	26	34	34	36	32	30	26	36	28	32	36	34	34
110010	32	34	28	30	34	32	38	36	30	40	34	36	28	34	32	30
110011	32	30	32	30	26	36	34	28	30	36	30	28	28	30	28	38
110100	32	28	34	38	32	36	30	34	38	30	36	36	30	30	32	32
110101	32	40	30	30	44	28	30	30	34	30	28	32	30	34	36	40
110110	32	30	32	34	28	30	20	34	26	32	30	32	26	28	30	36
110111	32	38	28	30	20	30	32	30	42	32	34	28	34	36	34	32
111000	32	32	32	40	38	30	38	30	28	36	32	32	34	34	30	30
111001	32	40	32	32	42	34	26	34	32	32	36	28	34	34	30	30
111010	32	38	30	32	34	36	28	34	28	30	30	36	26	32	32	34
111011	32	18	22	28	42	32	28	30	36	34	22	32	26	36	32	30
111100	32	32	32	36	24	32	32	28	28	36	36	32	28	36	36	32
111101	32	28	32	40	36	32	36	28	32	28	40	32	28	32	28	28
111110	32	38	34	32	28	30	26	36	28	30	30	32	28	26	34	32
111111	32	38	26	40	36	30	34	36	20	30	38	32	36	34	34	32

Πινακας 13. Ο πίνακας διατήρησης ισοτιμιών της συνάρτησης $\alpha_{S_3'} = \alpha_{S_3} \circ \varepsilon_Z$.

$\alpha_{S'_4}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000010	32	32	36	32	36	32	32	32	32	32	32	36	32	36	32	32
000011	32	28	32	40	32	32	40	28	28	24	32	32	24	32	28	32
000100	32	30	30	32	30	32	32	22	34	32	32	26	32	26	42	32
000101	32	34	30	28	34	32	28	38	34	36	32	22	36	42	38	32
000110	32	30	34	32	30	28	28	34	30	28	36	34	32	30	34	40
000111	32	30	30	36	30	44	32	30	34	32	44	34	36	34	34	32
001000	32	28	32	32	32	32	32	36	36	32	32	32	32	32	28	32
001001	32	32	28	24	36	32	40	32	32	24	32	36	40	28	32	32
001010	32	28	28	32	36	32	32	28	28	32	32	36	32	28	28	32
001011	32	36	28	32	28	32	32	28	28	32	32	28	32	28	36	32
001100	32	30	34	32	30	36	36	26	30	36	28	42	32	22	26	24
001101	32	30	30	28	30	36	32	22	34	32	36	26	28	26	42	32
001110	32	30	30	32	30	32	32	30	34	32	32	34	32	34	34	32
001111	32	34	30	36	34	32	36	30	34	28	32	30	28	34	30	32
010000	32	30	30	32	34	36	36	42	30	36	28	38	32	26	42	40
010001	32	34	30	28	30	28	32	26	30	32	28	42	28	42	38	32
010010	32	34	30	32	30	32	32	26	30	32	32	42	32	42	38	32
010011	32	34	34	28	30	32	36	22	34	28	32	26	36	38	22	32
010100	32	36	28	32	28	32	32	36	28	32	32	28	32	28	28	32
010101	32	36	36	40	28	32	32	36	36	32	32	36	24	28	36	32
010110	32	40	28	32	36	40	24	32	40	24	24	36	32	28	32	32
010111	32	36	40	40	40	32	32	28	28	32	32	32	40	32	36	32
011000	32	34	30	32	30	32	32	34	30	32	32	34	32	34	30	32
011001	32	34	34	36	30	32	28	30	34	36	32	34	28	30	30	32
011010	32	30	30	32	34	28	28	34	30	28	36	30	32	34	34	24
011011	32	34	30	20	30	36	32	34	30	32	36	34	20	34	30	32
011100	32	28	32	32	32	40	24	36	28	24	24	32	32	32	36	32
011101	32	32	28	24	28	32	32	32	32	32	32	36	24	36	32	32
011110	32	24	32	32	32	32	32	32	40	32	32	32	32	32	32	32
011111	32	32	24	40	40	32	32	32	32	32	32	32	24	32	32	32
100000	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100010	32	36	32	32	32	24	40	36	36	40	40	32	32	32	36	16
100011	32	32	36	32	36	32	32	32	32	32	32	36	32	36	32	32
100100	32	34	34	32	30	36	36	38	34	36	28	34	32	30	38	24
100101	32	30	34	36	34	28	32	30	34	32	28	38	36	38	34	32
100110	32	22	34	32	34	32	32	30	42	32	32	30	32	30	34	32
100111	32	30	22	36	42	32	36	34	30	28	32	30	28	34	34	32
101000	32	32	36	32	28	40	24	32	32	24	24	28	32	36	32	16
101001	32	28	32	32	32	32	32	36	36	32	32	32	32	32	28	32
101010	32	36	28	32	28	32	32	28	28	32	32	28	32	28	36	32
101011	32	36	36	32	28	32	48	36	36	16	32	28	32	36	36	32
101100	32	30	34	32	34	32	32	30	34	32	32	38	32	38	34	32
101101	32	30	30	28	34	32	28	26	30	36	32	30	36	34	26	32
101110	32	34	42	32	22	28	28	30	34	28	36	34	32	30	30	40
101111	32	22	34	28	34	20	32	30	42	32	20	30	28	30	34	32
110000	32	30	30	32	30	32	32	38	34	32	32	34	32	34	26	32
110001	32	34	30	28	34	32	36	30	34	28	32	38	36	26	30	32
110010	32	30	34	32	30	36	36	34	30	36	28	26	32	38	34	40
110011	32	30	30	36	30	36	32	38	34	32	36	34	36	34	26	32
110100	32	32	40	32	24	40	40	32	32	40	24	32	32	32	32	32
110101	32	24	32	32	32	40	32	32	40	32	40	32	32	32	32	32
110110	32	32	28	32	28	32	32	32	32	32	32	36	32	36	32	32
110111	32	36	32	40	32	32	32	28	36	32	32	32	24	32	28	32
111000	32	22	34	32	30	28	28	34	22	28	36	34	32	30	34	24
111001	32	30	22	44	22	28	32	30	34	32	28	34	44	34	34	32
111010	32	30	22	32	22	32	32	30	34	32	32	34	32	34	34	32
111011	32	42	30	36	34	32	28	30	42	36	32	30	28	34	30	32
111100	32	36	40	32	40	32	32	28	28	32	32	32	32	32	36	32
111101	32	24	36	40	28	32	32	32	24	32	32	28	24	36	32	32
111110	32	28	28	32	36	40	40	28	28	40	24	28	32	36	28	32
111111	32	36	28	32	28	24	32	36	28	32	24	28	32	28	28	32

Πινακας 14. Ο πίνακας διατήρησης ισοτιμιών της συνάρτησης $\alpha_{S'_4} = \alpha_{S_4} \circ \varepsilon_Z$.

$\alpha_{S'_5}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000010	32	36	30	34	30	34	28	32	36	32	34	30	34	30	32	28
000011	32	32	30	38	30	30	36	28	32	32	30	38	30	30	36	28
000100	32	34	30	32	32	34	30	32	32	34	34	36	28	30	30	32
000101	32	34	34	28	32	42	26	28	32	34	22	32	36	30	34	36
000110	32	30	28	26	30	28	34	32	32	30	32	30	26	24	34	32
000111	32	34	32	34	30	40	38	32	28	38	32	26	30	32	26	28
001000	32	32	34	38	32	32	30	26	30	34	36	20	34	38	28	36
001001	32	28	38	30	32	28	26	26	38	30	32	28	34	26	24	28
001010	32	36	32	32	30	26	34	34	34	34	30	34	36	28	28	32
001011	32	36	36	36	38	34	30	30	30	30	30	34	32	24	28	32
001100	32	34	32	30	32	34	36	42	30	36	30	24	30	36	26	28
001101	32	38	32	34	32	30	36	22	30	32	30	36	30	40	26	32
001110	32	30	30	32	30	36	32	34	30	32	36	34	28	38	30	28
001111	32	30	30	40	38	36	32	34	34	36	40	30	40	26	34	32
010000	32	34	30	32	32	30	26	24	32	30	30	28	32	34	42	12
010001	32	34	30	32	36	34	30	28	36	34	34	32	24	26	34	36
010010	32	30	32	30	34	28	30	24	36	38	36	38	30	36	26	32
010011	32	26	32	34	30	36	34	32	36	26	36	34	26	36	30	32
010100	32	36	28	32	32	32	32	32	28	28	36	36	32	36	28	32
010101	32	36	32	28	28	36	24	24	32	32	28	36	40	36	32	36
010110	32	32	38	38	34	30	36	32	36	32	38	34	34	34	32	32
010111	32	36	26	30	38	30	28	36	36	28	26	34	30	34	32	36
011000	32	38	32	34	36	22	28	34	34	32	30	32	34	36	30	28
011001	32	34	36	26	32	30	36	30	38	40	38	36	42	32	34	28
011010	32	34	34	24	30	36	32	34	30	32	36	34	32	30	30	32
011011	32	34	38	28	26	32	32	34	38	40	32	30	28	26	30	32
011100	32	32	30	34	36	32	26	34	30	38	28	32	34	30	32	32
011101	32	36	30	38	24	32	30	34	42	30	24	24	34	34	32	36
011110	32	28	24	32	30	30	30	34	30	34	30	38	36	36	36	32
011111	32	28	40	24	34	26	26	30	30	34	30	30	24	32	32	28
100000	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100010	32	28	30	34	30	34	28	40	28	32	26	38	34	30	16	20
100011	32	32	30	30	38	30	28	36	32	32	30	30	30	38	36	28
100100	32	30	38	36	32	38	30	36	36	26	30	36	32	46	34	32
100101	32	38	34	32	32	38	34	32	28	26	34	24	32	30	38	28
100110	32	34	36	30	30	32	34	28	36	30	28	30	38	32	30	32
100111	32	22	32	30	38	36	38	28	32	38	20	34	34	32	38	28
101000	32	36	30	30	32	36	26	34	34	26	36	32	38	30	28	32
101001	32	32	34	38	32	32	38	34	34	30	24	32	30	26	32	32
101010	32	32	28	24	38	38	38	26	38	34	30	30	24	36	28	36
101011	32	40	32	36	38	30	26	38	34	38	30	38	28	32	36	36
101100	32	34	36	26	32	26	32	38	30	28	34	28	30	36	38	32
101101	32	30	28	30	32	30	24	34	30	32	26	24	30	32	30	36
101110	32	38	34	28	38	36	36	30	22	24	32	30	36	30	34	32
101111	32	38	26	28	38	28	36	30	34	36	36	26	32	34	30	28
110000	32	34	30	32	28	26	30	28	36	34	34	32	32	34	34	36
110001	32	34	30	32	32	30	34	32	32	30	30	28	32	34	34	36
110010	32	38	32	30	30	40	34	36	32	42	32	34	30	36	34	32
110011	32	26	32	42	34	32	30	28	32	38	32	22	34	36	30	32
110100	32	32	20	36	28	32	36	24	28	32	28	32	28	28	32	32
110101	32	24	32	32	40	28	36	32	32	28	28	32	36	36	28	36
110110	32	36	30	26	30	30	40	32	36	28	30	30	38	34	28	32
110111	32	24	26	26	26	38	32	36	44	32	34	30	34	34	36	28
111000	32	34	36	26	32	30	36	30	26	36	26	32	38	36	30	32
111001	32	30	40	34	28	38	28	26	30	28	34	36	30	32	34	32
111010	32	38	22	32	34	36	32	30	38	28	32	34	36	30	30	28
111011	32	30	26	28	22	32	24	30	22	36	36	30	32	34	30	36
111100	32	24	26	30	32	28	34	34	26	34	36	32	42	30	36	36
111101	32	36	34	34	36	36	30	34	30	42	32	32	34	34	36	32
111110	32	28	36	28	34	34	30	34	34	30	30	30	36	28	32	36
111111	32	28	28	28	46	38	26	30	34	30	38	30	32	32	28	32

ΠΙΝΑΚΑΣ 15. Ο πίνακας διατήρησης ισοτιμιών της συνάρτησης $\alpha_{S'_5} = \alpha_{S_5} \circ \varepsilon_Z$.

$\alpha_{S_6'}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000010	32	32	32	32	34	26	34	26	34	38	30	34	28	32	32	36
000011	32	32	32	32	30	30	30	30	30	26	34	30	36	40	32	36
000100	32	32	34	30	34	30	40	32	34	34	32	36	36	40	38	30
000101	32	32	38	26	34	38	36	28	30	30	24	36	40	36	30	22
000110	32	36	30	30	32	32	34	30	32	32	30	34	24	36	34	34
000111	32	28	34	34	36	28	34	30	32	32	34	30	36	32	26	34
001000	32	34	30	32	28	30	30	24	34	32	40	38	38	28	32	30
001001	32	30	38	36	32	38	34	32	30	32	36	38	30	32	32	42
001010	32	34	34	36	34	36	24	34	32	34	30	32	26	28	36	30
001011	32	30	26	40	34	32	40	30	32	30	22	36	34	32	28	34
001100	32	30	32	34	34	28	34	40	28	30	32	30	30	28	34	36
001101	32	34	36	34	30	28	34	36	36	34	28	30	34	44	42	32
001110	32	34	32	38	28	34	28	30	30	32	30	28	26	40	34	36
001111	32	30	36	30	28	38	32	30	34	32	30	32	30	32	34	32
010000	32	34	32	30	32	34	28	18	28	30	28	26	32	34	20	42
010001	32	34	32	30	36	30	40	38	28	30	28	26	36	30	32	30
010010	32	34	32	30	30	32	34	24	26	40	30	40	28	34	36	30
010011	32	34	32	30	30	32	26	32	30	36	26	28	32	30	40	42
010100	32	30	34	32	34	28	28	30	30	28	28	34	28	30	26	28
010101	32	38	30	28	38	24	28	30	34	40	36	26	28	38	30	32
010110	32	26	38	32	36	34	26	32	32	30	30	36	32	34	30	32
010111	32	26	34	36	28	34	30	36	32	38	26	32	32	34	26	36
011000	32	32	30	34	32	32	30	34	30	34	36	28	34	30	32	32
011001	32	20	30	22	24	28	38	30	26	26	40	28	30	38	36	32
011010	32	40	34	30	34	34	28	32	32	24	38	34	30	30	28	32
011011	32	28	34	34	38	34	32	32	24	36	30	30	34	30	32	32
011100	32	32	32	32	30	26	34	30	32	28	36	40	34	26	34	34
011101	32	36	36	32	30	22	30	30	32	24	24	32	34	30	30	26
011110	32	36	40	28	28	28	32	32	30	34	30	26	38	30	34	34
011111	32	32	28	36	32	28	32	36	34	34	30	30	30	34	30	34
100000	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100010	32	36	32	28	30	34	30	42	34	26	30	46	32	32	36	44
100011	32	36	32	28	34	30	34	38	30	30	34	26	32	32	28	36
100100	32	32	30	34	30	34	32	24	30	30	32	28	36	32	42	34
100101	32	32	34	30	30	26	28	36	34	34	32	36	32	36	26	34
100110	32	40	34	38	32	36	38	38	28	32	38	30	36	36	26	30
100111	32	32	38	42	28	24	30	30	20	40	34	34	32	32	34	30
101000	32	34	34	28	32	34	30	32	30	36	32	30	38	20	36	34
101001	32	30	34	40	36	26	26	32	34	28	28	30	38	32	36	30
101010	32	38	30	36	34	32	28	34	28	26	30	28	30	36	36	34
101011	32	34	30	32	42	36	28	30	36	30	38	32	38	40	36	30
101100	32	30	40	26	34	36	34	32	36	30	32	22	30	28	34	36
101101	32	34	36	34	30	36	26	36	28	34	36	30	34	28	34	24
101110	32	38	24	26	32	26	32	30	38	36	30	32	38	32	30	36
101111	32	34	36	42	24	38	36	30	42	36	38	28	34	32	30	32
110000	32	34	32	30	32	34	36	26	32	34	32	30	28	30	40	30
110001	32	34	32	30	36	30	32	30	32	34	32	30	32	26	36	34
110010	32	30	32	34	34	24	30	32	30	24	34	32	20	30	36	26
110011	32	30	32	34	26	32	30	32	34	36	30	36	32	34	32	30
110100	32	30	30	36	30	32	28	30	30	28	32	30	40	34	34	36
110101	32	22	42	32	34	28	28	30	42	32	32	30	32	34	30	32
110110	32	22	26	32	28	38	30	32	32	26	26	28	32	30	34	32
110111	32	38	38	36	28	30	42	28	24	26	30	32	32	30	30	36
111000	32	32	26	38	36	36	30	26	30	26	40	32	30	34	32	32
111001	32	36	34	34	28	32	30	30	34	26	28	32	34	34	36	32
111010	32	36	38	30	26	30	24	32	32	28	34	34	38	34	32	32
111011	32	40	30	26	22	38	28	32	32	32	26	30	26	34	28	24
111100	32	32	32	32	30	34	34	38	28	32	32	28	30	38	30	30
111101	32	36	28	40	30	30	38	30	44	28	28	28	30	26	34	30
111110	32	32	24	32	40	36	28	32	26	34	26	34	38	34	34	30
111111	32	28	20	32	20	28	28	36	30	34	34	30	38	30	30	30

ΠΙΝΑΚΑΣ 16. Ο πίνακας διατήρησης ισοτιμιών της συνάρτησης $\alpha_{S_6'} = \alpha_{S_6} \circ \varepsilon_Z$.

$\alpha_{S'_7}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000010	32	32	34	26	36	28	34	34	34	34	32	32	30	30	32	32
000011	32	32	30	38	32	32	34	26	34	34	28	28	26	34	32	40
000100	32	32	34	34	32	28	26	30	36	36	42	34	36	32	26	38
000101	32	32	34	42	32	36	26	30	32	24	38	30	32	28	38	42
000110	32	36	32	28	24	32	36	28	30	26	30	34	38	30	34	26
000111	32	28	36	32	36	36	28	36	34	30	38	34	38	30	30	30
001000	32	28	32	36	30	30	30	38	28	36	32	32	30	34	34	30
001001	32	36	28	32	34	26	30	22	32	32	32	32	30	26	30	26
001010	32	32	30	22	34	30	28	32	34	38	32	36	32	32	34	34
001011	32	32	30	30	42	30	28	32	38	26	36	32	36	28	30	30
001100	32	32	30	30	34	26	32	32	32	28	30	34	30	26	36	32
001101	32	32	34	34	30	30	32	24	32	36	34	30	34	30	28	24
001110	32	32	32	32	34	34	38	30	30	26	26	38	28	24	28	32
001111	32	32	32	32	34	34	30	38	38	26	34	38	28	32	36	32
010000	32	30	34	36	32	30	30	32	30	36	36	38	30	28	40	18
010001	32	34	30	36	28	30	30	36	30	32	32	30	42	36	24	30
010010	32	30	32	34	28	34	28	22	32	30	32	18	36	26	36	30
010011	32	34	32	38	36	38	36	26	32	26	32	30	28	38	28	26
010100	32	34	40	38	32	22	36	30	38	40	30	28	30	28	34	36
010101	32	30	28	30	36	30	36	26	34	32	30	32	30	32	30	28
010110	32	30	34	28	24	34	34	32	32	30	30	32	32	26	30	36
010111	32	34	34	24	24	22	34	28	20	38	34	32	36	34	34	36
011000	32	34	30	28	34	32	28	38	34	40	32	26	32	34	34	24
011001	32	30	38	24	34	28	28	26	38	32	44	34	28	34	30	32
011010	32	30	32	34	30	32	30	36	32	34	28	34	34	32	30	32
011011	32	34	36	34	34	32	38	32	36	34	36	30	34	36	34	32
011100	32	34	32	30	30	40	34	32	34	32	38	32	28	34	36	30
011101	32	30	40	34	30	28	34	36	34	28	30	36	20	30	28	26
011110	32	34	38	28	30	32	36	34	40	30	30	32	34	32	32	34
011111	32	30	34	36	34	32	36	30	32	34	34	32	38	32	32	30
100000	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100010	32	32	34	34	28	36	26	34	34	34	32	24	30	30	16	24
100011	32	32	30	30	32	32	34	34	34	34	28	36	34	26	24	40
100100	32	32	30	38	32	36	30	34	28	36	30	38	36	32	30	34
100101	32	32	30	30	32	28	30	34	32	32	34	26	24	36	34	30
100110	32	28	28	32	24	32	24	32	38	34	34	38	30	30	30	30
100111	32	20	32	36	28	28	40	32	34	30	34	30	30	30	26	34
101000	32	32	28	36	30	26	26	30	36	24	28	40	38	46	30	30
101001	32	32	32	32	34	30	34	30	32	36	28	32	30	38	26	34
101010	32	28	34	30	34	34	32	32	26	34	36	36	32	28	30	34
101011	32	36	42	38	34	34	32	24	38	38	24	40	36	32	34	30
101100	32	36	38	34	34	30	32	44	32	32	30	30	38	22	36	28
101101	32	28	34	38	30	26	24	36	32	32	26	26	26	34	36	36
101110	32	36	32	36	26	30	38	34	30	30	34	34	36	36	36	28
101111	32	44	24	36	34	30	30	34	38	38	34	34	28	28	28	36
110000	32	34	34	32	36	38	34	32	30	40	36	34	34	36	28	34
110001	32	38	30	32	32	38	34	36	30	36	32	26	30	28	28	30
110010	32	34	32	38	32	26	32	30	32	34	32	38	32	26	32	30
110011	32	38	32	26	32	38	32	26	32	30	32	34	32	30	32	34
110100	32	30	36	30	28	38	36	34	30	36	34	36	26	36	34	32
110101	32	26	24	38	32	30	36	30	34	36	42	32	34	32	38	32
110110	32	34	30	36	28	34	26	28	24	34	34	40	28	26	30	32
110111	32	38	30	32	36	30	34	32	36	34	30	32	32	34	34	32
111000	32	34	26	32	30	36	36	30	34	32	36	30	28	30	34	32
111001	32	38	26	28	30	24	28	34	30	24	32	30	32	30	30	32
111010	32	38	36	30	34	36	22	28	32	34	24	30	30	36	38	32
111011	32	34	32	30	14	36	30	32	44	34	32	34	30	32	34	32
111100	32	26	40	30	34	36	22	28	26	32	30	32	32	30	32	34
111101	32	30	24	34	34	32	30	32	26	36	30	36	24	34	32	30
111110	32	26	38	28	34	28	32	30	32	30	30	32	30	36	28	30
111111	32	46	42	36	30	28	32	34	24	26	42	32	26	36	28	34

Πινακας 17. Ο πίνακας διατήρησης ισοτιμιών της συνάρτησης $\alpha_{S'_7} = \alpha_{S_7} \circ \varepsilon_Z$.

$\alpha_{S_8'}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
000010	32	34	32	30	30	32	34	32	30	32	30	36	28	30	32	38
000011	32	30	32	34	30	36	26	36	30	28	38	32	28	34	32	34
000100	32	30	30	32	32	34	30	28	34	32	36	30	38	32	32	46
000101	32	30	30	32	32	34	38	36	30	44	24	34	26	36	36	34
000110	32	32	34	34	34	38	32	28	36	36	34	34	34	30	36	24
000111	32	28	34	22	26	34	40	32	32	28	30	34	30	30	32	32
001000	32	32	34	30	32	32	34	30	30	34	32	32	34	30	36	28
001001	32	36	30	30	36	32	26	34	34	34	32	44	26	26	32	28
001010	32	34	30	32	34	36	28	30	32	30	30	36	38	28	32	30
001011	32	34	34	44	38	40	36	30	36	26	30	36	30	28	36	34
001100	32	30	32	30	32	34	32	26	32	34	28	22	32	38	36	26
001101	32	34	28	30	36	34	32	38	32	30	32	38	28	38	36	30
001110	32	32	32	36	30	34	34	34	30	26	34	34	36	36	36	32
001111	32	32	36	32	26	30	26	34	30	34	38	38	40	32	36	32
010000	32	32	32	32	32	32	32	24	32	32	32	32	32	24	32	16
010001	32	32	32	32	32	24	32	32	32	40	32	24	32	40	32	32
010010	32	34	32	30	30	32	34	40	30	32	30	36	28	38	32	22
010011	32	30	32	34	30	28	42	36	30	36	22	40	28	26	32	34
010100	32	30	26	28	36	30	30	28	30	36	28	30	30	32	36	34
010101	32	30	34	36	20	38	30	36	26	24	24	34	34	36	32	30
010110	32	32	38	22	30	26	32	28	40	32	26	34	26	30	32	36
010111	32	28	30	34	38	30	32	32	36	32	30	34	38	30	36	36
011000	32	28	34	34	32	36	34	34	38	30	32	28	34	34	28	24
011001	32	32	38	42	28	36	26	30	34	30	32	32	26	30	32	32
011010	32	30	38	28	26	32	28	34	32	34	30	32	38	32	32	34
011011	32	30	34	32	22	36	36	26	28	30	30	24	30	32	28	30
011100	32	26	28	30	36	34	32	38	36	34	36	34	40	34	32	26
011101	32	30	24	30	32	34	24	34	28	30	32	34	36	34	32	30
011110	32	28	28	36	34	34	34	30	34	26	26	30	28	32	32	32
011111	32	28	32	32	22	30	34	30	26	34	38	34	32	28	32	32
100000	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100001	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
100010	32	30	36	30	34	32	26	36	30	28	26	28	32	30	48	34
100011	32	34	28	34	34	28	26	40	30	32	26	24	32	26	24	30
100100	32	34	34	24	32	38	34	36	30	32	36	34	34	32	32	34
100101	32	34	34	24	32	38	26	28	34	36	32	30	30	28	28	30
100110	32	40	34	26	30	26	28	32	32	24	38	30	26	30	36	32
100111	32	28	26	30	22	30	28	36	36	32	34	38	30	30	32	32
101000	32	32	34	30	32	32	26	38	26	30	28	28	30	26	24	32
101001	32	36	30	30	36	32	34	26	30	30	28	40	38	38	20	32
101010	32	30	34	32	30	28	36	34	36	30	30	32	38	24	36	30
101011	32	22	30	28	34	40	36	34	24	34	38	32	30	32	32	34
101100	32	26	36	30	32	30	28	18	32	30	32	38	32	34	32	34
101101	32	30	32	30	36	30	28	30	24	34	28	30	36	26	40	30
101110	32	32	32	36	34	22	30	30	22	34	34	34	32	32	32	28
101111	32	40	28	32	30	42	30	30	30	42	38	30	28	28	32	36
110000	32	28	32	36	32	36	32	36	32	36	32	28	32	20	32	36
110001	32	36	32	28	32	36	32	36	32	36	32	28	32	28	32	28
110010	32	26	28	26	34	36	34	32	30	32	34	32	32	34	40	30
110011	32	38	36	38	34	32	34	36	30	36	34	28	32	38	32	34
110100	32	30	22	32	28	30	34	32	34	32	28	30	42	28	28	34
110101	32	38	30	32	28	30	34	32	38	36	32	34	38	32	32	30
110110	32	36	38	34	34	26	36	36	28	32	38	34	34	26	32	32
110111	32	32	38	38	26	30	28	32	32	40	26	34	38	34	36	32
111000	32	40	42	30	32	40	34	30	26	38	28	36	38	34	32	32
111001	32	36	30	30	28	32	26	34	38	30	28	32	30	38	36	32
111010	32	22	42	32	38	28	36	34	28	30	38	32	30	32	28	30
111011	32	38	30	28	34	32	36	34	24	26	30	32	38	32	32	34
111100	32	34	32	34	28	26	36	34	36	34	40	30	32	34	36	30
111101	32	30	44	26	40	34	28	38	36	30	28	30	36	34	28	34
111110	32	24	36	32	30	34	30	38	42	38	34	34	32	32	28	32
111111	32	24	32	36	34	30	22	30	26	38	30	38	28	36	28	32

ΠΙΝΑΚΑΣ 18. Ο πίνακας διατήρησης ισοτιμιών της συνάρτησης $\alpha_{S_8'} = \alpha_{S_8} \circ \varepsilon_Z$.

Βιβλιογραφία

[1] Ross Anderson, Eli Biham, and Lars Knudsen. *Serpent: A proposal for the Advanced Encryption Standard*, May 1998. AES candidate submission, available at the NIST site.

[2] Eli Biham. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991. Extended abstract in Advances in Cryptology, Proceedings of Crypto '90, pp. 2–21, 1990.

[3] Eli Biham and Adi Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, 1993.

[4] Eli Biham and Adi Shamir. Differential cryptanalysis of the full 16-round DES. In *Advances in Cryptology, Proceedings of Crypto '92*, volume 740 of *Lecture Notes in Computer Science*, pages 494–502, 1993.

[5] C. C. Cocks. A note on non-secret encyption. Research report, Communications-Electronics Security Group, November 1973. Available at the CESG site.

[6] Joan Daemen and Vincent Rijmen. *AES Proposal: Rijndael*, March 1999. AES candidate submission, available at the NIST site.

[7] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, November 1976.

[8] J. H. Ellis. The possibility of secure non-secret digital encyption. Research report, Communications-Electronics Security Group, January 1970. Available at the CESG site.

[9] J. H. Ellis. The history of non-secret encryption. Research report, Communications-Electronics Security Group, 1987. Available at the CESG site.

[10] H. Feistel. Cryptography and computer privacy. *Scientific American*, 228(5):15–23, May 1973.

[11] Martin E. Hellman. A cryptanalytic time–memory trade-off. *IEEE Transactions on Information Theory*, IT-26(4):401–406, July 1980.

[12] Neil F. Johnson and Sushil Jajodia. Exploring steganography: Seeing the unseen. *IEEE Computer*, 31(2):26–34, February 1998.

[13] Neil F. Johnson and Sushil Jajodia. Steganalysis: The investigation of hidden information. In *Proceedings of the IEEE Information Technology Conference,* Syracuse, New York, September 1st–3rd, pages 113–116, 1998.

[14] D. Kahn. *The Codebreakers. The Story of Secret Writing.* Macmillan, 1967.

[15] W. E. Madryga. A high performance encryption algorithm. In *Computer Security: A Global Challenge*, pages 557–570. North Holland: Elsevier Science Publishers, 1984.

[16] Mitsuru Matsui. The first experimental cryptanalysis of the Data Encryption Standard. In *Advances in Cryptology, Proceedings of Crypto '94*, volume 839 of *Lecture Notes in Computer Science*, pages 1–11, 1994.

[17] Mitsuru Matsui. Linear cryptanalysis method for the DES cipher. In *Advances in Cryptology, Proceedings of Eurocrypt '93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397, 1994.

[18] Ralph C. Merkle. Secure communications over insecure channels. *Communications of the ACM*, 21(4):294–299, April 1978.

[19] National Bureau of Standards, U.S. Department of Commerce. *Data Encryption Standard (DES)*, July 1977. Federal Information Processing Standards Publication 46, available at the NIST site.

[20] National Institute of Standards and Technology, U.S. Department of Commerce. *DES Modes of Operation*, December 1980. Federal Information Processing Standards Publication 81, available at the NIST site.

[21] National Institute of Standards and Technology, U.S. Department of Commerce. *Data Encryption Standard (DES)*, December 30 1993. Federal Information Processing Standards Publication 46-2, available at the NIST site.

[22] National Institute of Standards and Technology, U.S. Department of Commerce. *Announcing development of a Federal Information Processing Standard for Advanced Encryption Standard*, January 1997. Available at the NIST site.

[23] National Institute of Standards and Technology, U.S. Department of Commerce. *Announcing request for candidate algorithm nominations for the Advanced Encryption Standard (AES)*, September 1997. Available at the NIST site.

[24] National Institute of Standards and Technology, U.S. Department of Commerce. *Comments on proposed AES minimum acceptability requirements and evaluation criteria*, April 1997. Available at the NIST site.

[25] S. C. Pohling and M. E. Hellman. An improved algorithm for computing logarithms in GF(p) and its cryptographic significance. *IEEE Transactions on Information Theory*, 24(1):106–111, January 1978.

[26] Terry Ritter. Ritter's crypto glossary and dictionary of technical cryptogtaphy, January 1999. Available at Ritter's site.

[27] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.

[28] Ronald L. Rivest. The RC5 encryption algorithm. In B. Preneel, editor, *Fast Software Encryption*, volume 1008 of *Lecture Notes in Computer Science*, pages 86–96. Springer-Verlag, 1995. Available at the Rivest site.

[29] Ronald L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin. *The RC6 Block Cipher*, April 1998. AES candidate submission, available at the NIST site.

[30] Edward Roback and Morris Dworkin. First AES candidate conference. *Journal of Research of the NIST*, 104(1), January–February 1999. Available at the NIST site.

[31] M. J. B. Robshaw. Stream ciphers. Technical Report TR-701, RSA Laboratories, July 1995. Available at the RSA site.

[32] Bruce Schneier et al. *Twofish: A 128-Bit Block Cipher*, June 1998. AES candidate submission, available at the NIST site.

[33] C. E. Shannon. A mathematical theory of communication. *Bell Systems Technical Journal*, 27:379–423, 623–656, 1948.

[34] Douglas R. Stinson. *Cryptography. Theory and Practice.* Discrete Mathematics and Its Applications. CRC Press, 1995.

[35] M. J. Williamson. Non-secret encyption using a finite field. Research report, Communications-Electronics Security Group, January 1974. Available at the CESG site.

[36] M. J. Williamson. Thoughts on cheaper non-secret encryption. Research report, Communications-Electronics Security Group, August 1976. Available at the CESG site.

[37] Nevenko Zunic et al. *The MARS Encryption Algorithm*, August 1999. AES candidate submission, available at the NIST site.