4 ΚΡΥΠΤΟΓΡΑΦΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ

4.1. Εισαγωγή

Τα προηγούμενα κεφάλαια αποτελούν μια εισαγωγή στην κρυπτολογία, στις κατηγορίες κρυπτογραφικών πράξεων καθώς και στα βασικά μοντέλα κρυπτανάλυσης και αξιολόγησης της κρυπτογραφικής δύναμης ενός κρυπτοσυστήματος.

Στο κεφάλαιο αυτό θα διερευνήσουμε με περισσότερη λεπτομέρεια τις κρυπτογραφικές συναρτήσεις. Ως κρυπτογραφικές συναρτήσεις θεωρούμε τις συναρτήσεις αυτές οι οποίες έχουν κρυπτογραφικό ενδιαφέρον. Με άλλα λόγια, αναζητούμε συναρτήσεις που μπορούν να χρησιμοποιηθούν στην κατασκευή κρυπτογραφικών πράξεων ώστε το κρυπτοσύστημα που προκύπτει να μπορεί να προσφέρει τις κρυπτογραφικές υπηρεσίες που παρουσιάσαμε στο Κεφάλαιο 1.

Η βιβλιογραφία περιλαμβάνει μια μεγάλη ποικιλία κρυπτογραφικών συναρτήσεων. Ωστόσο, η έρευνα συνεχίζεται και είναι αναμενόμενο να ανακαλυφθούν επιπλέον συναρτήσεις (ή οικογένειες συναρτήσεων) οι οποίες να μπορούν να χρησιμοποιηθούν ως δομικά συστατικά κρυπτογραφικών πράξεων.

4.2. Ψευδοτυχαίες ακολουθίες

Το κυνήγι των τυχαίων αριθμών και γενικότερα των τυχαίων ακολουθιών θεωρείται μια από τις μεγαλύτερες προκλήσεις των θετικών επιστημών. Η ικανότητα επιλογής τυχαίων αριθμών είναι ένα κρίσιμο χαρακτηριστικό στην ασφάλεια των κρυπτοσυστημάτων. Η δημιουργία των κλειδιών περιλαμβάνει τυχαίες επιλογές από σύνολα στοιχείων τα οποία μπορεί να είναι τα ίδια τα κλειδιά, ή ποσότητες που καθορίζουν τα κλειδιά αυτά (όπως για παράδειγμα η τυχαία επιλογή ενός πρώτου αριθμού).

Είναι ίσως μάταιη η απόπειρα να χαρακτηρίσουμε έναν αριθμό από μόνο του ως «τυχαίο». Αν για παράδειγμα δώσουμε τον αριθμό 3526, κανείς δεν θα ήταν σε θέση να ορίσει αν αυτός ο αριθμός είναι τυχαίος. Παρόμοια, αν δώσουμε δύο αριθμούς 5 και 7, δεν θα μπορούσαμε να ισχυριστούμε ότι ο ένας είναι πιο τυχαίος από τον άλλον, ή ότι ο ένας είναι τυχαίος, ενώ ο άλλος δεν είναι.

Έτσι είναι πιο πρακτικό να αναφερόμαστε στην πηγή η οποία παράγει μια ακολουθία αριθμών και να εξετάσουμε το σύνολο των αριθμών αυτών. Βέβαια η οποιαδήποτε συστηματική εξέταση της ακολουθίας έρχεται σε δεοντολογική αντίφαση με τη φύση της έννοιας της τύχης. Είναι όμως αναγκαίο να κάνουμε κάποιους συμβιβασμούς προκειμένου να παραμετροποιήσουμε την τύχη και να καταλήξουμε στους ακόλουθους ορισμούς:

ΟΡΙΣΜΟΣ 4.1 – Μια ακολουθία αριθμών είναι ***ψευδοτυχαία*** όταν:

- περνά όλους τους γνωστούς στατιστικούς ελέγχους περί τυχαιότητας (στατιστική απαίτηση).
- η ακολουθία είναι απρόβλεπτη, δηλαδή δοθέντος ενός τμήματος της ακολουθίας αυτής είναι υπολογιστικά αδύνατο για τον αντίπαλο να καθορίσει τον αμέσως επόμενο αριθμό (κρυπτογραφική απαίτηση).

ΟΡΙΣΜΟΣ 4.2 – Μια ακολουθία αριθμών είναι ***πραγματικά τυχαία*** όταν:

- ικανοποιεί όλες τις απαιτήσεις του Ορισμού 4.1,
- δεν μπορεί να αναπαραχθεί με αξιοπιστία.

Ο Ορισμός 4.1 είναι και αυτός ο οποίος μας ενδιαφέρει περισσότερο στην κρυπτογραφία. Ο Ορισμός 4.2 διαχωρίζει τις μεθόδους παραγωγής ακολουθίας αριθμών με βάση της αξιοπιστία αναπαραγωγής. Δεχόμαστε δηλαδή, ότι μια πραγματικά τυχαία ακολουθία δεν μπορεί να αναπαραχθεί δεύτερη φορά, έστω και αν όλες οι αρχικές συνθήκες του «πειράματος» είναι ίδιες. Στην κρυπτογραφία μας ενδιαφέρει περισσότερο η αξιόπιστη παραγωγή τυχαίων ακολουθιών. Για παράδειγμα, στους κρυπταλγόριθμους ροής, η γεννήτρια κλειδοροής θα πρέπει να βασίζεται σε γεννήτρια ψευδοτυχαίων ακολουθιών. Επίσης, όπως θα δούμε σε επόμενη ενότητα, η ύπαρξη γεννητριών τυχαίων bits καθορίζει μια πολύ σημαντική οικογένεια κρυπτογραφικών πράξεων.

4.2.1. Στατιστικοί έλεγχοι τυχαιότητας

Στους στατιστικούς έλεγχους που θα παρουσιάσουμε θεωρούμε ότι η ακολουθία είναι δυαδική, αποτελείται δηλαδή από τα ψηφία **0** και **1**. Η μελέτη δυαδικών ακολουθιών προτιμάται γιατί στη σύγχρονη ψηφιακή πραγματικότητα οι ακολουθίες που παράγονται από ψηφιακά συστήματα βασίζονται στην ουσία σε δυαδικές ακολουθίες.

Ο έλεγχος της συχνότητας (frequency test)

Ο έλεγχος της συχνότητας είναι ο έλεγχος της υπόθεσης ότι το πλήθος των άσσων και των μηδενικών είναι το ίδιο, από στατιστικής πάντα άποψης. Έστω n_0 το πλήθος των μηδενικών σε μια ακολουθία και n_1 το πλήθος των άσσων στην ακολουθία αυτή. Το μήκος της ακολουθίας θα είναι $n_0 + n_1$. Από τη στατιστική, η κατανομή χ^2 μπορεί να χρησιμοποιηθεί για να ελεγχθεί η υπόθεση $n_0 = n_1$, για έναν βαθμό ελευθερίας:

$$\chi^2 = \frac{(n_0 - n_1)^2}{n}$$

Αν $n_0 \neq n_1$, τότε θεωρούμε ότι η πηγή μας είναι ***πολωμένη*** ή αλλιώς ***μεροληπτική***. Πιο συγκεκριμένα, αν $n_0 > n_1$, τότε η πηγή είναι πολωμένη προς τα μηδενικά, ενώ αν $n_0 < n_1$, τότε η πηγή είναι πολωμένη προς τους άσσους. Από κρυπτογραφικής πλευράς, η πόλωση μπορεί να προσδώσει πληροφορία η οποία μπορεί να χρησιμοποιηθεί από τον αντίπαλο.

Ο σειριακός έλεγχος (serial test)

Ο έλεγχος της συχνότητας είναι και ο πιο απλός στατιστικός έλεγχος που εφαρμόζεται σε μια δυαδική ακολουθία, όπου εξετάζεται η συχνότητα εμφάνισης των δυαδικών συμβόλων. Δεν εξετάζεται όμως η κατανομή αυτών μέσα στην ακολουθία. Για παράδειγμα, η ακολουθία [**00001111**] περνάει τον έλεγχο συχνότητας, αλλά ασφαλώς και δεν μπορεί να θεωρηθεί ψευδοτυχαία. Ο σειριακός έλεγχος είναι ένα επιπλέον βήμα που χρησιμοποιεί την κατανομή εναλλαγής των συμβόλων από **0** σε **1** και αντίστροφα, καθώς και τη διατήρηση των δυαδικών συμβόλων (από **1** σε **1** και από **0** σε **0**). Έστω n_{00}, n_{01}, n_{10} και n_{11} το πλήθος των **00, 01, 10** και **11** αντίστοιχα. Ο έλεγχος υπόθεσης:

$$n_{00} = n_{01} = n_{10} = n_{11} \approx \frac{n-1}{4}$$

πραγματοποιείται με την κατανομή χ^2 για δύο βαθμούς ελευθερίας. Έχει αποδειχθεί (Good, 1957) ότι η ποσότητα

$$\frac{4}{n-1}\sum_{i=0}^{1}\sum_{j=0}^{1} n_{ij}^2 - \frac{2}{n}\sum_{i=0}^{1} n_i^2 + 1$$

προσεγγίζει την χ^2 για δύο βαθμούς ελευθερίας. Επομένως, οι συχνότητες n_{ij} μπορούν να αντικατασταθούν στην παραπάνω σχέση.

Ο έλεγχος της αυτοσυσχέτισης (autocorrelation test)

Ο έλεγχος της αυτοσυσχέτισης (Beker & Piper, 1982) δείχνει αν τα δυαδικά σύμβολα είναι τυχαία διασπαρμένα μέσα στη δυαδική ακολουθία. Έστω η ακολουθία $[a_1 a_2 \ldots a_n]$. Ορίζεται η συνάρτηση $A(d)$, τέτοια ώστε:

$$A(d) = \sum_{i=1}^{n-d} a_i a_{i+d} \, .$$

Αν τα **0** και **1** είναι τυχαία διασπαρμένα μέσα στην ακολουθία, η αναμενόμενη τιμή του $A(d)$ θα είναι ίση με:

$$\mu = \frac{n_1^2 (n-d)}{n^2}$$

όπου n_1 το πλήθος των άσσων και $d \neq 0$. Ο στατιστικός έλεγχος υπόθεσης εδώ θα είναι για $A(d) = \mu$.

Τα κριτήρια του Golomb

Ο παραπάνω ορισμός της $A(d)$ προέρχεται από το γενικό ορισμό της αυτοσυσχέτισης:

$$C(d) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} a_i a_{i+d} \ .$$

Όταν η ακολουθία έχει περίοδο T, η αυτοσυσχέτιση θα είναι:

$$C_T(d) = \frac{1}{T} \sum_{i=1}^{T} a_i a_{i+d} \ .$$

Σε μια δυαδική ακολουθία οι τιμές των a_i ορίζονται από την αντιστοιχία $(0,1) \rightarrow (-1,1)$, προκειμένου να αποφευχθούν οι ακυρώσεις λόγου του πολλαπλασιασμού με το **0**. Με βάση τα παραπάνω, ο Golomb (1984) έθεσε τρία κριτήρια που πρέπει να πληροί μια ακολουθία προκειμένου να χαρακτηρισθεί ψευδοτυχαία:

Κριτήριο 1: Η διαφορά μεταξύ του πλήθους των μηδενικών και του πλήθους των άσσων θα πρέπει να είναι όσο το δυνατόν μικρότερη.

Κριτήριο 2: Ως ***διαδρομή*** ορίζεται η σειρά ομοίων συμβόλων η οποία περιβάλλεται από διαφορετικά σύμβολα. Τότε, σε μια περίοδο της ακολουθίας οι μισές από τις διαδρομές θα πρέπει να έχουν μήκος 1, το ένα τέταρτο των διαδρομών να έχουν μήκος 2, το ένα όγδοο 3, κ.ο.κ. Η ισχύς της συνθήκης αυτής εξετάζεται όσο ο αριθμός των διαδρομών είναι μεγαλύτερος ή ίσος από 2^l, όπου l το μήκος της διαδρομής.

Κριτήριο 3: Για $T \neq d$ η αυτοσυσχέτιση θα πρέπει να είναι σταθερή, ενώ για $d = 0$ ή $T = d$, η αυτοσυσχέτιση θα πρέπει να είναι ίση με 1.

ΠΑΡΑΔΕΙΓΜΑ 4.1 – Έλεγχος τυχαιότητας δυαδικής ακολουθίας. Έστω η ακολουθία [**110100111101000**], η οποία αναλύεται ως εξής:

ακολουθία	1	1	0	1	0	0	1	1	1	1	0	1	0	0	0
αντιστοιχία	1	1	-1	1	-1	-1	1	1	1	1	-1	1	-1	-1	-1
μήκη διαδρομών	2		1	1	2		4				1	1	3		

Η περίοδος είναι ίση με το μήκος της ακολουθίας, $T = 15$. Το πλήθος των άσσων είναι 8 ενώ το πλήθος των μηδενικών είναι 7. Η ακολουθία πληροί το κριτή-

ριο 1 διότι 8 – 7 = 1 είναι η μικρότερη διαφορά σε μια δυαδική ακολουθία περιττού μήκους.

Από τις 8 συνολικά διαδρομές, οι μισές (4) έχουν μήκος 1, το ένα τέταρτο (2) έχουν μήκος 2, ενώ το ένα όγδοο (1) έχουν μήκος 3. Για τη διαδρομή μήκους 4, είναι $8 < 2^4 = 16$, οπότε ο έλεγχος δεν μπορεί να εφαρμοστεί στη διαδρομή αυτή. Επομένως καταλήγουμε ότι η ακολουθία πληροί το κριτήριο 2.

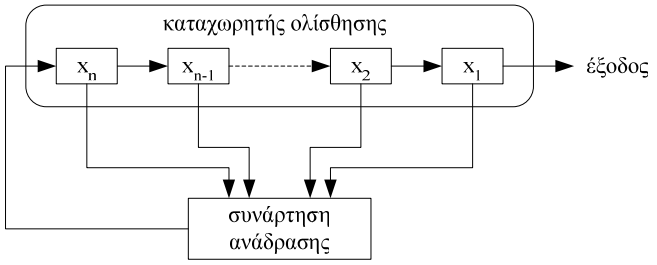
Τέλος, για $d = 0$ η αυτοσυσχέτιση είναι ίση με 1, ενώ για $d \neq T$ είναι σταθερή και ίση με -1/15. Συνεπώς η ακολουθία πληροί και το κριτήριο 3. Μπορούμε επομένως να δεχτούμε ότι η παραπάνω ακολουθία είναι μια ψευδοτυχαία δυαδική ακολουθία.

4.2.2. Γεννήτριες ψευδοτυχαίων ακολουθιών

Καταχωρητές ολίσθησης με ανάδραση

Οι καταχωρητές ολίσθησης (shift registers) έχουν μελετηθεί τις τελευταίες πέντε δεκαετίες. Ανήκουν στην κατηγορία των μηχανών πεπερασμένης κατάστασης (finite state machines). Μια μηχανή πεπερασμένης κατάστασης ορίζεται ως η συσκευή η ο οποία αποτελείται από έναν πεπερασμένο αριθμό καταστάσεων όπου η μεταπήδηση από τη μια κατάσταση στην άλλη ορίζεται από την υπάρχουσα κατάσταση και την είσοδο. Η είσοδος ορίζεται ως μια ακολουθία από ένα πεπερασμένο σύνολο στοιχείων. Η έξοδος μιας μηχανής πεπερασμένης κατάστασης είναι μια ακολουθία από ένα πεπερασμένο σύνολο στοιχείων. Οι ηλεκτρονικοί υπολογιστές είναι παραδείγματα μηχανών πεπερασμένης κατάστασης.

Οι καταχωρητές ολίσθησης με ανάδραση είναι αυτοί των οποίων η έξοδος τροφοδοτείται από μια συνάρτηση της οποίας το αποτέλεσμα τροφοδοτείται με τη σειρά του στην είσοδο του καταχωρητή, όπως φαίνεται στο Σχήμα 4.1.



Σχήμα 4.1 Καταχωρητής ολίσθησης με ανάδραση

Ο καταχωρητής ολίσθησης έχει την ικανότητα αποθήκευσης n δυαδικών στοιχείων (μνήμη των n bits). Ανά τακτά χρονικά διαστήματα, το κάθε στοιχείο αποθήκευσης x_i, μεταφέρει το περιεχόμενό του στο γειτονικό x_{i-1}. Το περιεχόμενο του x_1 παρουσιάζεται στην έξοδο της γεννήτριας, ενώ το x_n αποθηκεύει το αποτέλεσμα της συνάρτησης ανάδρασης με είσοδο το διάνυσμα $(x_1,x_2,\ldots,x_n)$.

Έστω $f:\{0,1\}^n \to \{0, 1\}$ η συνάρτηση ανάδρασης. Αν η f μπορεί να εκφραστεί με τη μορφή:

$$f(x_1, x_2, ..., x_n) = c_1x_1 + c_2x_2 + ... + c_nx_n \mod 2,$$

όπου οι σταθερές c_i είναι **0** ή **1**, η συνάρτηση είναι γραμμική, και η αντίστοιχη γεννήτρια ονομάζεται ***καταχωρητής ολίσθησης με γραμμική ανάδραση*** (linear feedback shift register).

Οι καταχωρητές ολίσθησης με γραμμική ανάδραση προτιμώνται στην κρυπτογραφία έναντι των μη γραμμικών, γιατί πέραν από το γεγονός ότι έχουν μελετηθεί σε μεγάλο βαθμό, υπάρχει μεθοδολογία για να παράγουν την ακολουθία με τη μέγιστη περίοδο. Η μέγιστη περίοδος ενός καταχωρητή με μνήμη n bits είναι ίση με 2^n-1 (εξαιρείται η κατάσταση όπου όλα τα x_i είναι μηδενικά). Η τιμή αυτή υπολογίζεται από το σύνολο όλων των δυνατών καταστάσεων του καταχωρητή, που είναι 2^n. Μέσα σε αυτές τις καταστάσεις συμπεριλαμβάνεται και η τιμή (0,0,…,0). Αν κάποια στιγμή εμφανισθεί η τιμή αυτή, τότε η γεννήτρια «κλειδώνει» και παράγει μόνο μηδενικά.

Για να αποφευχθεί η περίπτωση όπου ο καταχωρητής έχει μόνο μηδενικά, θα πρέπει να πληρούνται δύο προϋποθέσεις:

- Η αρχική τιμή του καταχωρητή να είναι διαφορετική της (0,0,…,0).
- Να επιλεγεί συνάρτηση ανάδρασης f τέτοια ώστε για οποιαδήποτε είσοδο $\mathbf{x} \neq (0,0,...,0)$, η $f(\mathbf{x})$ να μην παράγει n μηδενικά στη σειρά.

Η πρώτη προϋπόθεση είναι η προφανής απαίτηση να μην «φορτώσουμε» κατά την εκκίνηση του καταχωρητή το μηδενικό διάνυσμα. Αρχική τιμή απαιτείται διότι διαφορετικά δεν ορίζεται η είσοδος της συνάρτησης ανάδρασης.

Όσον αφορά τη δεύτερη προϋπόθεση, υπάρχει ένας σχετικά απλός τρόπος σύμφωνα με τον οποίο μπορούμε να επιλέξουμε τέτοια συνάρτηση ανάδρασης ώστε όχι μόνον να αποκλείσουμε την εμφάνιση της (0,0,..,0), αλλά και να παράγουμε όλες τις υπόλοιπες καταστάσεις του καταχωρητή. Στη συνέχεια θα περιγράψουμε τη μεθοδολογία επιλογής μιας συνάρτησης ανάδρασης με αυτό το επιθυμητό χαρακτηριστικό.

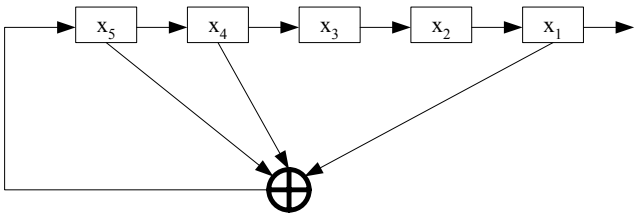
Μπορούμε να διαπιστώσουμε ότι η μορφή της γραμμικής συνάρτησης ανάδρασης καθορίζεται από τους συντελεστές c_1, c_2, …, c_n. Αν ο συντελεστής c_i είναι ίσος με 1, τότε το περιεχόμενο x_i, του καταχωρητή υπολογίζεται στο γραμμικό άθροισμα της συνάρτησης, ενώ στην περίπτωση που $c_i = 0$, το x_i παραλείπεται. Έτσι υπάρχουν 2^n δυνατές γραμμικές εξισώσεις, όσοι δηλαδή είναι και οι συνδυασμοί των σταθερών c_i. Η περιγραφή της συνάρτησης ανάδρασης μπορεί να γίνει με βάση τους συντελεστές με δύο τρόπους αναπαράστασης:

- με τη μορφή δυαδικής ακολουθίας, για παράδειγμα: **1011**, που σημαίνει ότι $c_1 = 1$, $c_2 = 0$, $c_3 = 1$, $c_4 = 1$, και

- με τη μορφή του χαρακτηριστικού πολυωνύμου, για παράδειγμα $f(x) = 1 + x + x^3 + x^4$.

ΠΑΡΑΔΕΙΓΜΑ 4.2 – Καθορισμός χαρακτηριστικού πολυωνύμου γραμμικής συνάρτησης ανάδρασης. Έστω η γεννήτρια του Σχήματος 4.2. Για να εκφράσουμε την ανάδραση με τη μορφή χαρακτηριστικού πολυωνύμου παρατηρούμε ότι: $c_1 = 1$, $c_2 = 0$, $c_3 = 0$, $c_4 = 1$, $c_5 = 1$. Έτσι το χαρακτηριστικό πολυώνυμο θα είναι:

$$f(x) = 1 + x + x^4 + x^5 .$$



Σχήμα 4.2 Καταχωρητής ολίσθησης ($n = 5$) με γραμμική ανάδραση.

Ο μέγιστος εκθέτης του πολυωνύμου καθορίζει το βαθμό αυτού. Για να παράγει ο καταχωρητής ολίσθησης με γραμμική ανάδραση την ακολουθία με τη μέγιστη περίοδο (2^n–1), θα πρέπει το χαρακτηριστικό πολυώνυμο της συνάρτησης ανάδρασης να πληροί τις ακόλουθες τέσσερις συνθήκες:

- να έχει βαθμό ίσο με το μέγεθος (τη μνήμη) του καταχωρητή, n,
- να είναι ανάγωγο (irreducible),
- να διαιρεί το $x^k + 1$, για $k = 2^n - 1$, και
- να μη διαιρεί το $x^k + 1$, για οποιοδήποτε $k < 2^n - 1$.

Το πολυώνυμο που πληροί τις παραπάνω συνθήκες ονομάζεται ***πρωτεύον*** (primitive).

ΠΑΡΑΔΕΙΓΜΑ 4.3 – Έλεγχος κριτηρίων του Golomb στις γεννήτριες καταχωρητών ολίσθησης με γραμμική ανάδραση. Έστω ότι ο καταχωρητής έχει μέγεθος n bit και ότι η συνάρτηση ανάδρασης έχει επιλεγεί ώστε η γεννήτρια να παράγει την ακολουθία με τη μέγιστη δυνατή περίοδο.

Το κριτήριο 1 απαιτεί η ακολουθία να έχει συγκρίσιμο πλήθος μηδενικών και άσσων. Επειδή η γεννήτρια παράγει το μέγιστο μήκος και ίσο με 2^n–1, στον καταχωρητή θα εμφανισθούν όλες οι τιμές εκτός από την τιμή (**0**, **0**, …, **0**). Από τις υπόλοιπες τιμές, το bit εξόδου x_1 θα είναι ίσο με **1** τις μισές φορές, και ίσο με **0** τις υπόλοιπες, δηλαδή:

$$n_1 = 2^{n-1} \text{ και } n_0 = 2^{n-1} - 1.$$

Επομένως:

$$n_1 - n_0 = 1.$$

Η διαφορά αυτή είναι και η ελάχιστη σε ένα σύνολο περιττού πλήθους δυαδικών στοιχείων.

Όσον αφορά το κριτήριο 2, αρκεί να δείξουμε ότι ο αριθμός των διαδρομών μήκους l είναι:

$$r(l) = \frac{r}{2^l},$$

όπου $r(l)$ ο αριθμός διαδρομών μήκους l και r ο συνολικός αριθμός των διαδρομών. Ο συνολικός αριθμός διαδρομών θα είναι:

$$r = \sum_{i=1}^{n} r(i).$$

Το παραπάνω άθροισμα το χωρίζουμε σε τρία επιμέρους αθροίσματα:

$$r = \sum_{i=1}^{n-2} r(i) + r(n-1) + r(n)$$

τα οποία αντιπροσωπεύουν τις περιπτώσεις όπου $0 < l < n - 1$, l = n – 1 και $l = n$. Ο διαχωρισμός αυτός βοηθάει τον υπολογισμό του r.

Στην περίπτωση που $l = n$, έχουμε μόνο μια διαδρομή που σημαίνει ότι όλες οι θέσεις του καταχωρητή έχουν αποθηκευμένο το ίδιο σύμβολο. Επειδή όμως η τιμή (**0**, **0**, …, **0**) εξαιρείται, δεχόμαστε ότι ο καταχωρητής έχει την τιμή (**1**, **1**, …, **1**). Επομένως $r(n) = 1$.

Στην περίπτωση που $l = n$-1, βρίσκουμε ότι είναι δυνατή μόνο μια ακολουθία. Από την προηγούμενη περίπτωση, εφόσον δεχόμαστε ότι υπάρχει η διαδρομή με n άσσους, τότε θα πρέπει να περικλείεται από δύο μηδενικά, ένα στην αρχή και ένα στο τέλος. Οι αντίστοιχες και μοναδικές δύο τιμές του καταχωρητή για να δημιουργηθεί η ακολουθία αυτή είναι οι (**0**, **1**, **1**, …, **1**) και (**1**, **1**, …, **1**, **0**), με την τιμή (**1**, **1**, …, **1**) να παρουσιάζεται ενδιάμεσα. Συνεπώς διαδρομή μήκους n-1 άσσων δεν μπορεί να υπάρξει, αφού καταναλώνεται στη δημιουργία της μεγαλύτερης διαδρομής μήκους n. Αντίθετα, η διαδρομή με $n - 1$ μηδενικά προκύπτει από τις διαδοχικές τιμές του καταχωρητή (**1**, **0**, …, **0**) και (**0**, …, **0**, **1**). Έτσι προκύπτει ότι $r(n - 1) = 1$.

Στην περίπτωση όπου $0 < l < n - 1$ υποθέτουμε ότι έχουμε μια διαδρομή αποτελούμενη από l άσσους. Τότε η διαδρομή ακολουθείται από ένα μηδενικό, οπότε οι θέσεις που απομένουν επιτρέπουν 2^{n-l-2} τιμές. Παρόμοια, σε μια διαδρομή αποτελούμενη από l μηδενικά, ακολουθεί ένας άσσος και οι εναπομείναντες θέσεις επιτρέπουν 2^{n-l-2} τιμές. Συνολικά θα είναι:

$$r(l) = 2^{n-l-2} + 2^{n-l-2} = 2^{n-l-1}$$

και το πλήθος των διαδρομών προκύπτει:

$$r = \sum_{l=1}^{n-2} 2^{n-l-1} + 2 = 2^{n-1}.$$

Επειδή όμως $r(l) = 2^{n-l-1}$, έπεται ότι:

$$r(l) = r2^{-l}.$$

Τέλος, όσον αφορά το κριτήριο 3, για $d = T$ η αυτοσυσχέτιση θα είναι:

$$C_T(d) = \frac{1}{T}\sum_{i=1}^{T} a_i^2 = 1,$$

ενώ για $d \neq T$:

$$C_T(d) = \frac{1}{T}\sum_{i=1}^{T} a_i a_{i+d} = \frac{1}{T}(n_0 - n_1) = -\frac{1}{2^n - 1}.$$

Γραμμική πολυπλοκότητα

Η γραμμική πολυπλοκότητα (linear complexity) είναι μια μέτρηση η οποία εφαρμόζεται στις γεννήτριες ψευδοτυχαίων ακολουθιών που βασίζονται σε καταχωρητές ολίσθησης με γραμμική ανάδραση.

ΟΡΙΣΜΟΣ 4.3 – Έστω η ακολουθία $\mathbf{a} = [a_1, a_2, \ldots]$ και έστω $\mathbf{a}^n$ τα n πρώτα bits της ακολουθίας αυτής. Ως ***γραμμική πολυπλοκότητα*** της $\mathbf{a}^n$ ονομάζουμε τον ελάχιστο αριθμό στοιχείων, συμβολικά $\mathrm{LC}(\mathbf{a}^n)$, ενός καταχωρητή ολίσθησης, που απαιτούνται για να παραχθεί η ακολουθία $\mathbf{a}^n$.

Από τον ορισμό της γραμμικής πολυπλοκότητας απορρέουν οι παρακάτω ιδιότητες:

- Για κάθε $n \geq 1$, ισχύει $0 \leq \mathrm{LC}(\mathbf{a}^n) \leq n$.
- Αν η ακολουθία είναι η μηδενική, $\mathbf{a} = [0, 0, 0, \ldots]$, τότε $\mathrm{LC}(\mathbf{a}^n)=0$, για κάθε $n \geq 1$.
- $\mathrm{LC}(\mathbf{a}^n) = n$ αν και μόνο αν $\mathbf{a}^n = [0, 0, 0, \ldots, 0, 1]$.
- Αν δεν υπάρχει καταχωρητής ολίσθησης με γραμμική ανάδραση ο οποίος να μπορεί να παράγει την ακολουθία $\mathrm{LC}(\mathbf{a}^n)$, τότε $\mathrm{LC}(\mathbf{a}^n)=\infty$.
- Αν η ακολουθία $\mathbf{a}$ είναι περιοδική με περίοδο T, τότε $\mathrm{LC}(\mathbf{a}^n) \leq T$.

Ο τρόπος υπολογισμού της γραμμικής πολυπλοκότητας εξαρτάται από το χαρακτηριστικό πολυώνυμο της γραμμικής συνάρτησης ανάδρασης και πιο συγκεκριμένα από το αν αυτό είναι ανάγωγο. Στην περίπτωση που το χαρακτηριστικό

πολυώνυμο είναι ανάγωγο, τότε η γραμμική πολυπλοκότητα είναι ίση με το βαθμό του χαρακτηριστικού πολυωνύμου.

Ασφάλεια καταχωρητών ολίσθησης με γραμμική ανάδραση

Αν και οι καταχωρητές ολίσθησης με γραμμική πολυπλοκότητα μπορούν να παράγουν ψευδοτυχαίες ακολουθίες με ελεγχόμενη περίοδο, ένας αντίπαλος μπορεί να προσδιορίσει το κλειδί και τη συνάρτηση ανάδρασης με σχετικά μικρό αριθμό στοιχείων της κλειδοροής. Για την ακρίβεια, για έναν καταχωρητή ολίσθησης με μνήμη των *l* bits, αρκούν μόνο *2l* bits κλειδοροής για να μπορέσει να ανακαλύψει ο αντίπαλος το χαρακτηριστικό πολυώνυμο της γραμμικής συνάρτησης ανάδρασης. Στην περίπτωση που ο αντίπαλος προσδιορίσει το χαρακτηριστικό πολυώνυμο, θα είναι στη θέση να κατασκευάσει μια ίδια γεννήτρια και να προβλέψει τη συνέχεια της ακολουθίας πέραν των *2l* bits που κατέχει.

Η κρυπταναλυτική επίθεση η οποία προσδιορίζει το χαρακτηριστικό πολυώνυμο μιας δυαδικής ακολουθίας είναι γνωστή ως αλγόριθμος των Berlekamp και Massey (1969) που περιγράφεται στη συνέχεια.

Προσδιορισμός χαρακτηριστικού πολυωνύμου δυαδικής ακολουθίας

Η βασική ιδέα του αλγόριθμου είναι ότι θεωρούμε ότι μας αποκαλύπτονται διαδοχικά τα bits της δυαδικής ακολουθίας, οπότε σε κάθε βήμα μπορούμε να προσδιορίσουμε καλύτερα είτε τη μορφή του πολυωνύμου, ή το απαιτούμενο μέγεθος του καταχωρητή ολίσθησης.

Με το πρώτο bit μπορούμε να κατασκευάσουμε ένα αρχικό πολυώνυμο, το οποίο είναι ουσιαστικά ίσο με τη μονάδα. Επίσης θεωρούμε ότι ο καταχωρητής είναι μηδενικού μήκους αν το bit είναι ίσο με **0**, ή μήκους ενός bit, αν το bit της ακολουθίας είναι ίσο με **1**. Στη συνέχεια δοκιμάζουμε την ικανότητα της κατασκευής μας να προβλέψει το επόμενο bit. Δηλαδή, υπολογίζουμε την επόμενη τιμή και ελέγχουμε αν αυτή συμπίπτει με το δεύτερο bit της αρχικής μας δυαδικής ακολουθίας. Στην περίπτωση που συμπίπτει, δε χρειάζεται να κάνουμε αλλαγές στην κατασκευή μας. Στην περίπτωση που δεν συμπίπτει, ελέγχουμε αν χρειάζεται να αυξήσουμε το μέγεθος του καταχωρητή ολίσθησης και επαναπροσδιορίζουμε το χαρακτηριστικό πολυώνυμο αυξάνοντας το βαθμό του.

Το βασικό εργαλείο που μας βοηθάει στις παραπάνω αποφάσεις της αύξησης του μεγέθους του καταχωρητή ή/και τον επαναπροσδιορισμό του χαρακτηριστικού πολυωνύμου, είναι η γραμμική πολυπλοκότητα. Όπως αναφέρθηκε, η γραμμική πολυπλοκότητα είναι ίση με το βαθμό του πρωτεύοντος χαρακτηριστικού πολυωνύμου. Επομένως, σε όλη τη διάρκεια της εφαρμογής του αλγόριθμου είμαστε σε θέση να γνωρίζουμε τη γραμμική πολυπλοκότητα της ακολουθίας, και να παρακολουθούμε την αύξησή της.

Στη συνέχεια παραθέτουμε τον αλγόριθμο των Berlekamp και Massey για τον προσδιορισμό του χαρακτηριστικού πολυωνύμου που αντιστοιχεί σε μια δυαδική ακολουθία $\mathbf{a}^n = [a_0, a_1, ..., a_{n-1}]$

1. Αρχικές τιμές:
   $f(x) \leftarrow 1$, χαρακτηριστικό πολυώνυμο
   $b(x) \leftarrow 1$, προσωρινή μεταβλητή
   $l \leftarrow 0$, μέγεθος καταχωρητή ολίσθησης
   $N \leftarrow 0$, μετρητής
   $m \leftarrow -1$, προσωρινή αποθήκευση μετρητή
2. Αν $N = n - 1$ τότε πήγαινε στο (10).
3. Υπολόγισε τη διαφορά της πρόβλεψης από την ακολουθία:
   $$d = a_N + \sum_{i=0}^{l-1} c_i a_{N+i-l}$$
4. Υπάρχει διαφορά; Αν όχι, ($d = 0$) τότε πήγαινε στο (9)
5. Αν ναι, ($d = 1$) τότε:
   $f'(x) \leftarrow f(x)$ αποθήκευσε το πολυώνυμο
   $f(x) \leftarrow f(x) + b(x)x^{N-m}$ υπολόγισε τη νέα μορφή
6. Το μέγεθος του καταχωρητή είναι μεγαλύτερο του $\frac{N}{2}$;
7. Αν ναι, ($l > \frac{N}{2}$) τότε πήγαινε στο (9).
8. Αν όχι, ($l \le \frac{N}{2}$) τότε:
   $l \leftarrow N + 1 - l$ αύξησε το μέγεθος του καταχωρητή ανάλογα
   $b(x) \leftarrow f'(x)$ αποθήκευσε το παλιό πολυώνυμο
   $m \leftarrow N$ αποθήκευσε την τρέχουσα τιμή του N.
9. Αύξησε το $N \leftarrow N + 1$ και πήγαινε στο (2)
10. Το χαρακτηριστικό πολυώνυμο είναι το $f(x)$. Τέλος!

Κατά τον τερματισμό του ο αλγόριθμος καταλήγει με τις μεταβλητές l και $f(x)$ να περιέχουν το μέγεθος του καταχωρητή ολίσθησης και το χαρακτηριστικό πολυώνυμο αντίστοιχα. Αυτές οι δύο παράμετροι καθορίζουν πλήρως έναν καταχωρητή ολίσθησης με γραμμική ανάδραση.

Το βήμα (6) του αλγόριθμου είναι ίσως το πιο σημαντικό και χρειάζεται περαιτέρω ανάλυση. Αρχικά, από τη συνθήκη που εξετάζεται στο βήμα (6) φαίνεται η απαίτηση να κατέχει ο αντίπαλος τουλάχιστο $2l$ bits της δυαδικής ακολουθίας. Η συνθήκη εκφράζεται ισοδύναμα ως $2l > N$.

Ο λόγος $N/2$ είναι επίσης μια σημαντική τιμή. Αν προβάλλουμε τις τιμές της γραμμικής πολυπλοκότητας κατά τη διάρκεια του αλγόριθμου, θα παρατηρήσουμε ότι αντιστοιχούν σε μια αύξουσα συνάρτηση, η οποία ακολουθεί την τιμή $N/2$. Έστω η συνάρτηση LC($\mathbf{a}^n$) η οποία ορίζεται από την ακολουθία των γραμμικών

πολυπλοκοτήτων LC($\mathbf{a}^i$), $i = 0,1,2,...,n-1$. Τότε η συνάρτηση LC($\mathbf{a}^n$) ονομάζεται ***προφίλ πολυπλοκότητας*** (complexity profile) της ακολουθίας $\mathbf{a}^n$. Έχει αποδειχθεί ότι το προφίλ πολυπλοκότητας μιας πραγματικά τυχαίας δυαδικής ακολουθίας μήκους N bits είναι η ευθεία $N/2$, όπως φαίνεται στο Σχήμα 4.4. Έτσι και στον αλγόριθμο των Berlekamp και Massey, η συνθήκη ελέγχου του μήκους του καταχωρητή ολίσθησης συγκρίνει το υπάρχον μήκος του καταχωρητή και αυξάνεται στη περίπτωση που το μήκος αυτό είναι μικρότερο από αυτό μιας πραγματικά τυχαίας ακολουθίας. Για την ακρίβεια, το μήκος αυξάνεται με τρόπο ώστε να είναι όσο το δυνατόν πλησιέστερα στην τιμή $N/2$.

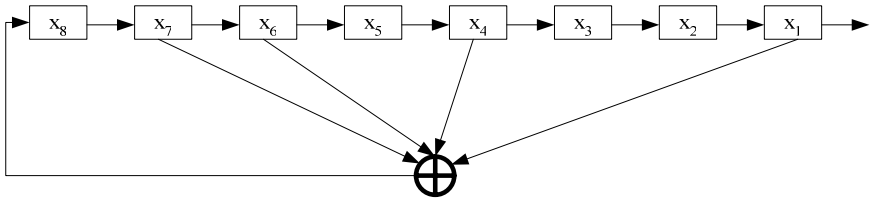
ΠΑΡΑΔΕΙΓΜΑ 4.4 – Καθορισμός γεννήτριας καταχωρητή ολίσθησης με γραμμική ανάδραση και προφίλ πολυπλοκότητας δυαδικής ακολουθίας. Έστω η ακολουθία $a^{14} = [1,0,0,1,1,1,0,0,1,0,0,0,0,1]$. Τα αποτελέσματα των βημάτων του αλγόριθμου καθορισμού του χαρακτηριστικού πολυωνύμου συνοψίζονται στον Πίνακα 4.1.

N	a_N	d	$f(x)$	$b(x)$	l	m
0	1	1	$1+x$	1	1	0
1	0	1	1	1	1	0
2	0	0	1	1	1	0
3	1	1	$1+x^3$	1	3	3
4	1	1	$1+x+x^3$	1	3	3
5	1	0	$1+x+x^3$	1	3	3
6	0	0	$1+x+x^3$	1	3	3
7	0	0	$1+x+x^3$	1	3	3
8	1	0	$1+x+x^3$	1	3	3
9	0	0	$1+x+x^3$	1	3	3
10	0	1	$1+x+x^3+x^7$	$1+x+x^3$	8	10
11	0	0	$1+x+x^3+x^7$	$1+x+x^3$	8	10
12	0	0	$1+x+x^3+x^7$	$1+x+x^3$	8	10
13	1	1	$1+x+x^4+x^6+x^7$	$1+x+x^3+x^7$	8	10

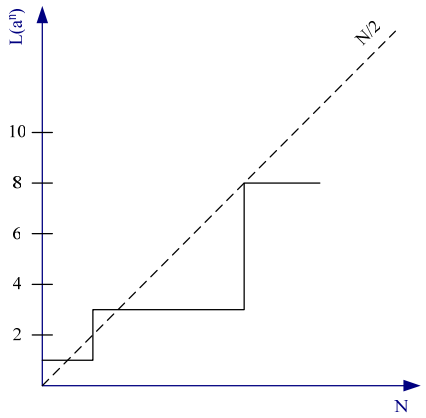
Πίνακας 4.1 Κρυπτανάλυση της $a^{14} = [1,0,0,1,1,1,0,0,1,0,0,0,0,1]$.

Από τον πίνακα μπορούμε να εξάγουμε το προφίλ πολυπλοκότητας το οποίο αντιστοιχεί στη στήλη του μεγέθους l του καταχωρητή. Στο Σχήμα 4.4 παρουσιάζεται το προφίλ πολυπλοκότητας σε αντιπαράθεση με την ευθεία $N/2$ που ταυτίζεται με το προφίλ πολυπλοκότητας μιας πραγματικά τυχαίας ακολουθίας.

Το χαρακτηριστικό πολυώνυμο βρέθηκε να είναι το $1+x+x^4+x^6+x^7$, ενώ το μέγεθος του καταχωρητή είναι 8 bit. Με αυτές τις πληροφορίες, μπορούμε να κατασκευάσουμε τη γεννήτρια, όπως φαίνεται στο Σχήμα 4.3.



Σχήμα 4.3 Κατασκευή γεννήτριας της $a^{14} = [1,0,0,1,1,1,0,0,1,0,0,0,0,1]$



Σχήμα 4.4 Προφίλ πολυπλοκότητας της ακολουθίας.

Κρυπτανάλυση με γνωστό μέγεθος καταχωρητή

Πολλές φορές στην πράξη οι γεννήτριες υλοποιούνται με τυποποιημένα μεγέθη καταχωρητών, που είναι συνήθως δυνάμεις του 2. Έτσι, αν ο αντίπαλος γνωρίζει το σύστημα το οποίο χρησιμοποιείται για τη δημιουργία της ψευδοτυχαίας δυαδικής ακολουθίας, τότε μπορεί να προσδιορίσει τη γραμμική συνάρτηση ανάδρασης. Όπως και στην προηγούμενη μέθοδο, ο αντίπαλος χρειάζεται $2l$ bits της κλειδοροής, προκειμένου να εφαρμόσει την κρυπταναλυτική επίθεση στη γεννήτρια (όπου l το μέγεθος του καταχωρητή).

Η αρχή της κρυπτανάλυσης είναι η ίδια με αυτήν της κρυπτανάλυσης του κρυπτοσυστήματος του Hill. Ο αντίπαλος καλείται να προσδιορίσει τις τιμές των σταθερών συντελεστών c_i της συνάρτησης ανάδρασης. Το πλήθος των σταθερών είναι ίσο με το μέγεθος του καταχωρητή, επομένως απαιτούνται l γραμμικές εξι-

σώσεις με l αγνώστους, τους συντελεστές c_i. Για οποιοδήποτε στοιχείο a_i της ακολουθίας με $i > l$, ισχύει:

$$a_i = \sum_{j=0}^{l-1} c_j a_{i-l+j} \mod 2$$

δηλαδή κάθε στοιχείο προσδιορίζεται από τα l προηγούμενα στοιχεία. Επειδή χρειάζονται l σχέσεις για να μπορεί να λυθεί το σύστημα με τους l αγνώστους, έπεται ότι απαιτούνται τα a_0, a_1, …, a_{l-1} καθώς και τα a_l, a_{l+1}, …, a_{2l-1} που εμφανίζονται στην αριστερή πλευρά της παραπάνω εξίσωσης. Το γραμμικό σύστημα μπορεί να εκφρασθεί στην αλγεβρική μορφή:

$$(a_l, a_{l+1}, ..., a_{2l-1}) = (c_0, c_1, ..., c_{l-1}) \begin{pmatrix} a_0 & a_1 & \cdots & a_{l-1} \\ a_1 & a_2 & \cdots & a_l \\ \vdots & \vdots & \ddots & \vdots \\ a_{l-1} & a_l & \cdots & a_{2l-2} \end{pmatrix}$$

με αγνώστους τα $(c_0, c_1, ..., c_{l-1})$. Το σύστημα θα έχει λύση αν ορίζεται ο

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{l-1} \\ a_1 & a_2 & \cdots & a_l \\ \vdots & \vdots & \ddots & \vdots \\ a_{l-1} & a_l & \cdots & a_{2l-2} \end{pmatrix}^{-1} .$$

Καταχωρητές ολίσθησης με μη γραμμική συνάρτηση ανάδρασης

Όσον αφορά τους καταχωρητές ολίσθησης με μη γραμμική ανάδραση, οι απόψεις σχετικά με τη κρυπτογραφική τους δύναμη διίστανται. Από τη μια, η συστηματική ανάλυση και μαθηματική τεκμηρίωση που επικρατεί στους καταχωρητές με γραμμική ανάδραση απουσιάζει στην περίπτωση των καταχωρητών με μη γραμμική συνάρτηση ανάδρασης. Έτσι η ασφάλεια που μπορεί να παρέχει ένας καταχωρητής με μη γραμμική συνάρτηση ανάδρασης δεν είναι αντικειμενικά μετρήσιμη. Από την άλλη όμως, η μη γραμμικότητα είναι ένα σημαντικό χαρακτηριστικό που επιζητούμε στην κρυπτογραφία και στους κρυπταλγόριθμους ειδικότερα, για να παρέχουν υψηλή σύγχυση. Επομένως, η ίδια η μη γραμμικότητα μπορεί να αποτελέσει εγγύηση της ισχύος του καταχωρητή.

Οι βασικές διαφορές με τους καταχωρητές με γραμμική ανάδραση είναι:

- Στις μη γραμμικές συναρτήσεις επιτρέπεται η μηδενική τιμή (0, 0, …, 0) στον καταχωρητή ολίσθησης.
- Η συνάρτηση ανάδρασης μπορεί να αποτελείται από περισσότερες από μία συναρτήσεις οι οποίες είναι πεπλεγμένες μεταξύ τους με ποικίλους τρό-

πους.

- Το πλήθος των μη γραμμικών συναρτήσεων είναι κατά πολλές τάξεις μεγαλύτερο του πλήθους των γραμμικών συναρτήσεων.

Σε αντίθεση με τις γραμμικές συναρτήσεις όπου κυριαρχεί μόνον η πράξη της πρόσθεσης (mod 2), στην περίπτωση των μη γραμμικών συναρτήσεων οι l είσοδοι που αντιστοιχούν στις μονάδες αποθήκευσης του καταχωρητή μπορούν να συνδυασθούν και με την πράξη του πολλαπλασιασμού. Στα διακριτά μαθηματικά μια τέτοια συνάρτηση με l εισόδους και μια έξοδο του ενός bit ονομάζεται Μπουλιανή (Boolean). Υπάρχουν συνολικά 2^{2^l} διαφορετικές Μπουλιανές συναρτήσεις, για l μεταβλητές. Ο αριθμός αυτός είναι αρκετά μεγαλύτερος του αριθμού των γραμμικών συναρτήσεων που είναι της τάξης του 2^l. Ωστόσο, έχει δειχθεί ότι ένας καταχωρητής μήκους l και με μη γραμμική Μπουλιανή συνάρτηση μπορεί να παράγει δυαδική ακολουθία η οποία θα έχει μέγιστη περίοδο ίση με 2^l.

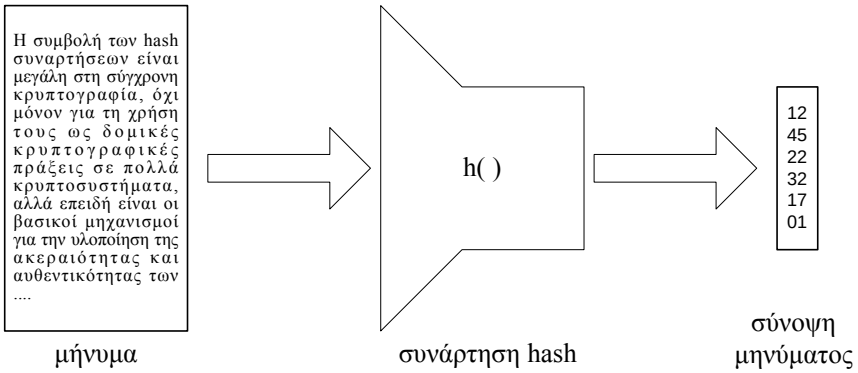
4.3. Μονόδρομες hash συναρτήσεις

Η συμβολή των hash συναρτήσεων είναι μεγάλη στη σύγχρονη κρυπτογραφία, όχι μόνον για τη χρήση τους ως δομικές κρυπτογραφικές πράξεις σε πολλά κρυπτοσυστήματα, αλλά επειδή είναι οι βασικοί μηχανισμοί για την υλοποίηση της ακεραιότητας και αυθεντικοποίησης των δεδομένων.

ΟΡΙΣΜΟΣ 4.4 – Μια συνάρτηση hash $h: \mathcal{F}^* \to \mathcal{G}^n$ αντιστοιχίζει ένα στοιχείο $x \in \mathcal{F}^*$ αυθαίρετου μήκους, στο στοιχείο $y \in \mathcal{G}^n$ με συγκεκριμένο μήκος n:

$$y = h(x).$$

Η σχηματική παράσταση μιας συνάρτησης hash φαίνεται στο Σχήμα 4.5. Η συνάρτηση δέχεται ένα συγκριτικά μεγάλο μήνυμα και παράγει μια ***σύνοψη*** του μηνύματος, μικρότερου και συγχρόνως σταθερού μεγέθους.



Σχήμα 4.5 Μια συνάρτηση hash

ΟΡΙΣΜΟΣ 4.5 – Μια κρυπτογραφική συνάρτηση hash είναι μια συνάρτηση hash με τις ακόλουθες ιδιότητες:

1. δοθέντος y, είναι υπολογιστικά αδύνατο να βρεθεί x τέτοιο ώστε $h(x) = y$
2. δοθέντων x, $h(x)$, είναι υπολογιστικά αδύνατο να βρεθεί x' τέτοιο ώστε $h(x') = h(x)$
3. είναι υπολογιστικά αδύνατο να βρεθούν $x_1, x_2 \in \mathcal{F}^*$, τέτοια ώστε, $h(x_1) = h(x_2)$.

Στην πράξη υπάρχει περίπτωση, ανάλογα με την εφαρμογή, να απατούνται μόνον ορισμένες από τις ιδιότητες των κρυπτογραφικών hash συναρτήσεων. Έτσι, ορίζονται οικογένειες κρυπτογραφικών hash συναρτήσεων με παρόμοιες ιδιότητες. Πιο συγκεκριμένα, οι συναρτήσεις οι οποίες διατηρούν τις ιδιότητες (1) και (2), ονομάζονται ***μονόδρομες hash συναρτήσεις*** (one-way hash functions), ενώ οι συναρτήσεις που διατηρούν τις ιδιότητες (2) και (3) ονομάζονται ***ανθεκτικές σε συγκρούσεις hash συναρτήσεις*** (collision resistance hash functions). Σύγκρουση ονομάζουμε την περίπτωση όπου περισσότερα από ένα στοιχεία του πεδίου ορισμού της συνάρτησης αντιστοιχίζεται στο ίδιο στοιχείο του συνόλου τιμών. Όπως είναι αναμενόμενο, σε ένα στοιχείο του συνόλου τιμών αντιστοιχούν περισσότερο από ένα στοιχεία του πεδίου ορισμού, αφού το σύνολο τιμών είναι πεπερασμένο, ενώ το πεδίο ορισμού είναι μη πεπερασμένο. Μια hash συνάρτηση είναι ανθεκτική σε συγκρούσεις όταν δεν υπάρχει συστηματικός τρόπος – πέραν της εξαντλητικής αναζήτησης – να ανακαλύπτονται στοιχεία που να καταλήγουν στην ίδια σύνοψη. Η ιδιότητα (3) συμπεριλαμβάνει την ιδιότητα (2), αφού η ιδιότητα (2) είναι πιο περιοριστική της (3)˙ εφόσον είναι υπολογιστικά αδύνατο να βρεθούν δύο οποιεσδήποτε τιμές οι οποίες έχουν την ίδια σύνοψη, τότε είναι ακόμη πιο δύσκολο να βρεθεί μια δεύτερη τιμή που να έχει την ίδια σύνοψη με μια δεδομένη τιμή. Έτσι, η ιδιότητα (2) ονομάζεται και ***ασθενής αντίσταση σε συγκρούσεις*** ενώ η ιδιότητα (3) ονομάζεται ***ισχυρή αντίσταση σε συγκρούσεις***.

Η ύπαρξη των μονόδρομων συναρτήσεων δεν έχει αποδειχθεί. Αυτό σημαίνει ότι δεν μπορούμε να ισχυριστούμε με μαθηματική εγγύηση αν μια συνάρτηση είναι μονόδρομη. Επιπλέον, μια συνάρτηση που θεωρείται σήμερα μονόδρομη, μπορεί στο μέλλον να αποδειχθεί ότι δεν είναι. Οι εξελίξεις στα θεωρητικά και εφαρμοσμένα μαθηματικά εισάγουν ένα βαθμό αβεβαιότητας. Μια μελλοντική ανακάλυψη μπορεί να προτείνει μεθόδους οι οποίες λύνουν «άλυτα» προβλήματα με «υπολογιστικά εφικτούς» τρόπους. Παρόλα αυτά, τα περισσότερα σενάρια στην κρυπτογραφία βασίζονται στην ύπαρξη των μονόδρομων συναρτήσεων.

Η έννοια του κλειδιού υφίσταται και στις μονόδρομες hash συναρτήσεις. Μάλιστα θα διαχωρίσουμε τις μονόδρομες συναρτήσεις σε δύο κατηγορίες, στις συναρτήσεις άνευ κλειδιού και στις συναρτήσεις με κλειδί. Οι συναρτήσεις άνευ κλειδιού καλύπτονται από τον Ορισμό 4.5.

ΟΡΙΣΜΟΣ 4.6 – Μια μονόδρομη hash συνάρτηση με κλειδί ορίζεται ως η συνάρτηση $h_k : \mathcal{F}^* \rightarrow \mathcal{G}^n$, όπου για κάθε $k \in \boldsymbol{K}$, υπάρχει μια μονόδρομη hash συνάρτηση που να αντιστοιχίζει το $:\mathcal{F}^*$ στο $\mathcal{G}^n$.

ΠΑΡΑΔΕΙΓΜΑ 4.5 – Δημιουργία μονόδρομης hash συνάρτησης με κλειδί, από μονόδρομη hash συνάρτηση άνευ κλειδιού. Έστω η μονόδρομη συνάρτηση $h:\mathcal{F}^*\rightarrow\mathcal{G}^n$. Εφόσον δεν υπάρχει ουσιαστικός περιορισμός στο σύνολο ορισμού της συνάρτησης, ορίζουμε την $h_k : \mathcal{F}^* \rightarrow \mathcal{G}^n$, έτσι ώστε:

$$h_k(x) = h(x \,\|\, k),$$

όπου $x \,\|\, k$ το μήνυμα που προκύπτει από την αλληλουχία των x και k. Παρόμοια θα μπορούσε να ορισθεί η μονόδρομη συνάρτηση ως:

$$h_k(x) = h(k \,\|\, x),$$

δηλαδή με το κλειδί να προηγείται του μηνύματος. Έχει αποδειχθεί ότι η σειρά της αλληλουχίας του κλειδιού με το μήνυμα είναι σημαντική από πλευράς ασφάλειας. Πιο συγκεκριμένα, έχει αποδειχθεί ότι η δεύτερη μονόδρομη συνάρτηση του παραδείγματος είναι πιο ασφαλής από την πρώτη, επειδή παρεμβάλλεται περισσότερη πληροφορία μεταξύ του κλειδιού και του τελικού αποτελέσματος, που ενδεχομένως είναι διαθέσιμο στον αντίπαλο.

4.3.1. Μέγεθος της σύνοψης

Η επιτυχία εύρεσης συγκρούσεων σε μια συνάρτηση hash εξαρτάται τόσο από το σχεδιασμό των μετασχηματισμών της συνάρτησης, όσο και από το μέγεθος της σύνοψης. Για παράδειγμα, στην εκφυλισμένη περίπτωση όπου η σύνοψη έχει μέγεθος ίσο με 1 bit, αναμένουμε τα μισά μηνύματα να αντιστοιχίζονται στην τιμή **0** και τα υπόλοιπα στην τιμή **1.** Συνεπώς η επιλογή ενός επαρκούς μεγέθους της σύνοψης για να αποτρέψει τις συγκρούσεις είναι ένα σημαντικό βήμα στον καθορισμό μιας συνάρτησης hash.

Το «παράδοξο των γενεθλίων»

Το παράδοξο των γενεθλίων (birthday paradox) είναι ένα κλασσικό πρόβλημα στη θεωρία των πιθανοτήτων το οποίο χρησιμοποιείται για να δώσει διάσταση στο πρόβλημα της επιλογής του μεγέθους της σύνοψης. Στη βιβλιογραφία έχει επικρατήσει ο όρος «παράδοξο» που αναφέρεται στη διαστρεβλωμένη αντίληψη που έχουμε για την εκτίμηση ορισμένων μεγεθών. Συνήθως το μέγεθος που επιλέγουμε με βάση την αντίληψή μας είναι πολύ μικρότερο από την πραγματικότητα, όπως θα δείξουμε με το ακόλουθο πρόβλημα.

Έστω ότι 25 άτομα παρευρίσκονται σε μια δεξίωση. Αν αναλογισθούμε την πιθανότητα δύο από αυτά να έχουν την ίδια ημέρα γενέθλια (σε διαφορετικό ή ίδιο έτος), τότε μάλλον εκτιμάμε ότι η πιθανότητα αυτή βρίσκεται κοντά στην τιμή 25/365 δηλαδή κοντά στο 7%. Στην πραγματικότητα, η πιθανότητα να έχουν δύο

από τα 25 άτομα γενέθλια την ίδια ημέρα είναι μεγαλύτερη του 50%. Αυτό υπολογίζεται (θεωρώντας χάριν απλότητας ότι δεν υπάρχουν δίσεκτα έτη) ως εξής.

Παραμετροποιούμε το πρόβλημα θεωρώντας *n* άτομα σε ένα χώρο και θέλουμε να υπολογίσουμε την πιθανότητα να έχουν οποιαδήποτε 2 άτομα γενέθλια την ίδια ημέρα. Αν η πιθανότητα αυτή είναι p_n, τότε η πιθανότητα να μην έχουν οποιαδήποτε 2 άτομα γενέθλια την ίδια μέρα θα είναι

$$p'_n = 1 - p_n .$$

Αρκεί λοιπόν να υπολογίσουμε την p'_n.

Έστω ότι τα άτομα εισέρχονται διαδοχικά στην αίθουσα της δεξίωσης. Η πιθανότητα του πρώτου ατόμου να μην έχει γενέθλια με κανένα από τα άτομα της αίθουσας είναι 1 ή 365/365, αφού δεν υπάρχει κανένα άλλο. Στη συνέχεια εισέρχεται το δεύτερο άτομο. Η πιθανότητα του δεύτερου ατόμου να μην έχει γενέθλια με το πρώτο, είναι (365-1)/365. Θα πρέπει δηλαδή τα γενέθλιά του να είναι μια από τις υπόλοιπες 364 μέρες του χρόνου. Παρόμοια, το τρίτο άτομο θα πρέπει να «επιλέξει» μεταξύ των 365-2 διαθέσιμων τιμών που δεν αντιστοιχούν στα γενέθλια των δύο προηγουμένων. Επομένως η πιθανότητα θα είναι ίση με

$$p'_3 = \frac{365}{365} \cdot \frac{(365-1)}{365} \cdot \frac{(365-2)}{365}$$

Όταν το *n*-στό άτομο εισέλθει στην αίθουσα, η πιθανότητα να μην έχει γενέθλια με κανένα από τα προηγούμενα άτομα, θα δίνεται από την

$$\begin{aligned} p'_n &= \frac{365}{365} \cdot \frac{(365-1)}{365} \cdot \frac{(365-2)}{365} \cdot \ldots \cdot \frac{(365-n+1)}{365} \\ &= \frac{365!}{(365-n)!365^n} \end{aligned}$$

Επομένως,

$$p_n = 1 - \frac{365!}{(365-n)!365^n}.$$

Από την παραπάνω σχέση προκύπτει ότι για *n* = 23, η πιθανότητα είναι $p_{23} = 0{,}507$. Δηλαδή για 23 άτομα (πόσο μάλλον για 25) η πιθανότητα είναι μεγαλύτερη του 50% να έχουν γενέθλια δύο από αυτά την ίδια μέρα. Αυτός ο αυστηρός μαθηματικός υπολογισμός έρχεται αντίθετος με την αντίληψή μας.

Το παράδοξο των γενεθλίων πρέπει να λαμβάνεται υπόψη στην επιλογή του μεγέθους της σύνοψης. Ανάλογη με την πιθανότητα των γενεθλίων δύο ατόμων, είναι και η πιθανότητα δύο μηνύματα να έχουν το ίδιο αποτέλεσμα σε μια συνάρτηση hash. Αντιπροσωπευτικά μεγέθη σύνοψης των κρυπτογραφικών hash είναι 128 και 160 bits. Σε πολλές εφαρμογές 128 bits θεωρούνται αρκετά, λαμβάνοντας

υπόψη ότι το μήνυμα που συνοψίζεται έχει αρκετή περίσσεια (Κεφ. 3), ώστε οι τυχόν συγκρούσεις να αντιστοιχούν σε μη έγκυρα μηνύματα. Ωστόσο, κατά τη συγγραφή του βιβλίου αυτού, 160 bits είναι η αποδεκτή τιμή για την αποφυγή συγκρούσεων.

Σε ένα σχήμα επικοινωνίας, ο αντίπαλος όσον αφορά την ακεραιότητα του μηνύματος μπορεί να είναι και η Αλίκη ή ο Βύρων, όπως θα δούμε παρακάτω στο Παράδειγμα 4.8.

4.3.2. Αυθεντικοποίηση και ακεραιότητα ενός μηνύματος

Όπως αναφέρθηκε στην εισαγωγή της ενότητας των hash συναρτήσεων, οι συναρτήσεις αυτές μπορούν να προσφέρουν αυθεντικοποίηση και ακεραιότητα των δεδομένων. Οι οικογένειες των κρυπτογραφικών hash συναρτήσεων που χρησιμοποιούνται στην αυθεντικοποίηση και στην ακεραιότητα κατατάσσονται στις κατηγορίες των κωδικών αυθεντικοποίησης μηνυμάτων και των κωδικών ανίχνευσης τροποποίησης.

ΟΡΙΣΜΟΣ 4.7 – Ο ***κώδικας αυθεντικοποίησης μηνύματος*** (Message Authentication Code, MAC) είναι μια μονόδρομη κρυπτογραφική hash συνάρτηση με κλειδί, η οποία προσφέρει ασθενή αντίσταση σε συγκρούσεις:

- δοθέντων x, $h_k(x)$, είναι υπολογιστικά αδύνατο να βρεθεί x' τέτοιο ώστε $h_k(x') = h_k(x)$.

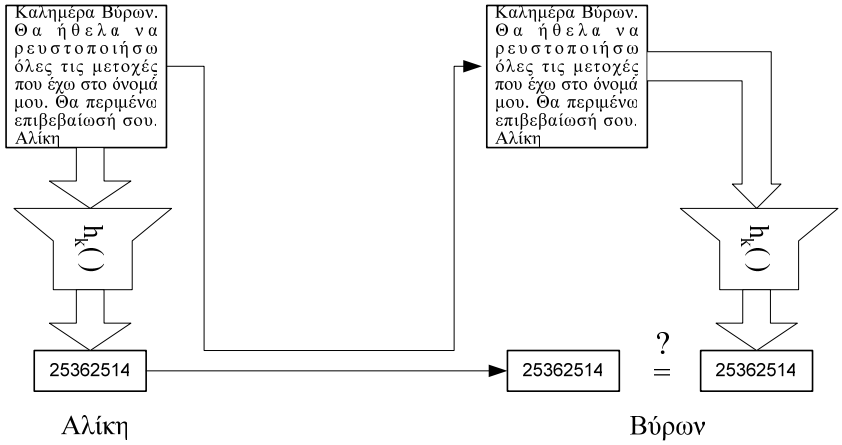
ΟΡΙΣΜΟΣ 4.8 – Ο ***κώδικας ανίχνευσης τροποποίησης*** (Modification Detection Code, MDC) είναι μια μονόδρομη κρυπτογραφική hash συνάρτηση άνευ κλειδιού, η οποία προσφέρει ασθενή αντίσταση σε συγκρούσεις:

- δοθέντων x, $h(x)$, είναι υπολογιστικά αδύνατο να βρεθεί x' τέτοιο ώστε $h(x') = h(x)$.

Η επιλογή μεταξύ του MAC και του MDC εξαρτάται από τις συγκεκριμένες συνθήκες της εφαρμογής καθώς και την υπόθεση της επίθεσης του αντιπάλου. Ο MAC αφορά περισσότερο δύο μέλη τα οποία επικοινωνούν άμεσα και οι πληροφορίες ανταλλάσσονται και προς τις δύο κατευθύνσεις. Στην περίπτωση που απαιτείται υψηλός βαθμός ακεραιότητας ενώ η εμπιστευτικότητα είναι χαμηλή, η Αλίκη και ο Βύρων μπορούν να χρησιμοποιήσουν ένα πρωτόκολλο ανταλλαγής μυστικού κλειδιού που θα χρησιμοποιηθεί στον υπολογισμό του MAC. Το κάθε μήνυμα που ανταλλάσσεται συνοδεύεται από τον αντίστοιχο MAC. Μόλις ο Βύρων λάβει το μήνυμα και το MAC, υπολογίζει ανεξάρτητα το MAC και ελέγχει αν είναι το ίδιο με το MAC που έχει λάβει. Αν οι δύο συνόψεις συμπίπτουν, τότε το μήνυμα που έλαβε είναι ακριβώς αυτό που έστειλε η Αλίκη. Η διαδικασία παρουσιάζεται στο Σχήμα 4.6.

Παράδειγμα περίπτωσης όπου απαιτείται μεγάλη ακεραιότητα και χαμηλή εμπιστευτικότητα είναι στα σήματα ελέγχου των μέσων μαζικής μεταφοράς. Η πληροφορία που φτάνει για παράδειγμα σε έναν πύργο ελέγχου αεροπορικής κυ-

κλοφορίας θα πρέπει να είναι ακριβής και σωστή, γιατί στην αντίθετη περίπτωση ο χάρτης των θέσεων των αεροπλάνων δε θα συμπίπτει με την πραγματικότητα. Παρόμοια, τα σήματα ελέγχου των γραμμών των τρένων και οι εντολές αλλαγής των «ψαλιδιών» στις σιδηροδρομικές γραμμές δεν απαιτούν εμπιστευτικότητα, αλλά η αυθαίρετη αλλαγή αυτών μπορεί να προκαλέσει ατυχήματα.



Σχήμα 4.6 Έλεγχος ακεραιότητας με MAC

Η χρήση του MDC συναντάται σε ασύμμετρη επικοινωνία, στις περιπτώσεις όπου ένας στέλνει ένα μήνυμα σε πολλούς. Στο Διαδίκτυο αυτό συναντάται συχνά στη λήψη ηλεκτρονικών αγαθών όπως ηλεκτρονικά βιβλία, λογισμικό κτλ. Όταν μια εταιρεία λογισμικού για παράδειγμα ανακοινώνει τη διάθεση αναβαθμίσεως του λογισμικού της, μπορεί να δημοσιεύσει τον αντίστοιχο MDC σε εφημερίδα, περιοδικό, ή γενικότερα σε κάποιο δημόσια διαθέσιμο μέσο. Ο πελάτης μπορεί να «κατεβάσει» το λογισμικό από το δικτυακό τόπο της εταιρείας και για να ελέγξει ότι το λογισμικό είναι ακριβώς αυτό που έχει προσφέρει η εταιρεία, υπολογίζει τον MDC και τον συγκρίνει με αυτόν που έχει δημοσιευθεί. Επειδή δεν υπάρχει κλειδί στο σχήμα αυτό, ο έλεγχος μπορεί να πραγματοποιηθεί από οποιονδήποτε πελάτη.

Όπως αναφέρουμε συχνά στο βιβλίο, η κρυπτογραφία δε λύνει το πρόβλημα αλλά το μετασχηματίζει σε μορφή τέτοια ώστε η διαχείριση του προβλήματος να είναι πιο αποτελεσματική. Με βάση το σκεπτικό αυτό, παρουσιάζουμε ένα πρωτόκολλο ελέγχου ακεραιότητας ενός εγγράφου μεταξύ της Αλίκης και του Βύρωνα:

0. Η Αλίκη επιθυμεί να στείλει στον Βύρωνα ένα πολυσέλιδο έγγραφο όσο το δυνατόν γρηγορότερα. Η λύση να το στείλει διαβάζοντάς το μέσω τηλεφώνου δεν επαρκεί. Το τηλέφωνο προσφέρει ακεραιότητα επειδή ο Βύρων γνωρίζει τη φωνή της Αλίκης, επομένως είναι αδύνατο κάποιος αντίπαλος να αλλάξει τα λόγια της. Η Αλίκη και ο Βύρων αποφασίζουν να εκμεταλλευτούν την ακεραιότητα που προσφέρει η τηλεφωνική επικοινωνία ως εξής:

1. Η Αλίκη υπολογίζει τον MDC του εγγράφου και στη συνέχεια στέλνει με ηλεκτρονικό ταχυδρομείο το έγγραφο στον Βύρωνα.
2. Μόλις παραλάβει το έγγραφο ο Βύρων υπολογίζει τον MDC του εγγράφου.
3. Ο Βύρων τηλεφωνεί την Αλίκη και της εκφωνεί το αποτέλεσμα (σύνοψη) του υπολογισμού του MDC.
4. Η Αλίκη επιβεβαιώνει αν η σύνοψη του Βύρωνα ταυτίζεται με τη σύνοψη που έχει υπολογίσει η ίδια.

Η Αλίκη και ο Βύρων μπορούν να συμφωνήσουν μέσω της τηλεφωνικής επικοινωνίας για τον αλγόριθμο MDC που θα χρησιμοποιήσουν. Έτσι, ενώ αρχικά η απαίτηση να μεταδοθεί το έγγραφο μέσω τηλεφώνου προκειμένου να εξασφαλισθεί υψηλή ακεραιότητα, μετασχηματίζεται στη μετάδοση ενός μικρότερου μηνύματος μέσω τηλεφώνου, με τον ίδιο βαθμό ασφάλειας.

ΠΑΡΑΔΕΙΓΜΑ 4.6 – Εφαρμογή του παραδόξου των γενεθλίων στην πλαστογραφία μηνύματος (Yuval, 1979). Σε αυτό το παράδειγμα αντίπαλος είναι η Αλίκη, παρόλο που επικοινωνεί με τον Βύρωνα για την υπογραφή κάποιου συμβολαίου. Η Αλίκη κλείνει μια συμφωνία με τον Βύρωνα και αναλαμβάνει να ετοιμάσει το αντίστοιχο συμβόλαιο για να το υπογράψει ο Βύρων.

1. Στην πραγματικότητα η Αλίκη ετοιμάζει δύο συμβόλαια, ένα όπως συμφώνησε με τον Βύρωνα και ένα ευνοϊκότερο για αυτήν και λιγότερο για τον Βύρωνα. Οι γνώσεις του Βύρωνα σχετικά με κρυπτογραφία δεν είναι αρκετές, οπότε η Αλίκη επιλέγει MDC ο οποίος υποκύπτει σε επίθεση εύρεσης συγκρούσεων.
2. Η Αλίκη υπολογίζει τη σύνοψη του αρχικού συμβολαίου και με βάση την τιμή αυτή, κάνει μικρές και ασήμαντες αλλαγές στο δεύτερο συμβόλαιο, προκειμένου να πετύχει μια σύνοψη ίδια με αυτήν του πρώτου συμβολαίου.
3. Η Αλίκη στέλνει το πρώτο συμβόλαιο στον Βύρωνα, ο οποίος υπολογίζει ανεξάρτητα τη σύνοψη αυτού και την υπογράφει (κρυπτογραφεί τη σύνοψη με το ιδιωτικό του κλειδί).
4. Ο Βύρων στέλνει την υπογεγραμμένη σύνοψη στην Αλίκη, η οποία καταστρέφει το πρώτο συμβόλαιο και επισυνάπτει την υπογραφή του Βύρωνα στο δεύτερο. Σε τυχόν διαφωνία, η Αλίκη είναι σε θέση να παρουσιάσει το δεύτερο συμβόλαιο που φαινομενικά έχει υπογραφεί από τον Βύρωνα.

Από το παράδειγμα φαίνεται ότι η απαίτηση να πληρούνται οι κρυπτογραφικές ιδιότητες μιας συνάρτησης hash εξαρτάται τόσο από την εφαρμογή, όσο και από την υπόθεση της επίθεσης του αντιπάλου. Μπορούμε να ταξινομήσουμε τις ευκαιρίες, ικανότητες και στόχους του αντιπάλου, ως προς τις MAC και MDC, όπως φαίνεται στον Πίνακα 4.2.

κατηγορία μονόδρομης hash	στόχοι αντιπάλου	ευκαιρίες/ικανότητες
MAC	Εντοπισμός κλειδιού	πλαστογραφία
	Εντοπισμός x', τέτοιου ώστε για δεδομένο x είναι $h_k(x) = h_k(x')$ (με το κλειδί γνωστό στον αντίπαλο)	επίθεση γνωστού κειμένου, x, $h_k(x)$
	Εντοπισμός δύο x και x', έτσι ώστε $h_k(x) = h_k(x')$ (με το κλειδί άγνωστο στον αντίπαλο)	επίθεση επιλεγμένου κειμένου, x, $h_k(x)$
MDC	Εντοπισμός x', τέτοιου ώστε για δεδομένο x είναι $h(x) = h(x')$	επίθεση γνωστού κειμένου, x, $h(x)$
	Εντοπισμός δύο x και x', έτσι ώστε $h(x) = h(x')$	επίθεση επιλεγμένου κειμένου, x, $h(x)$

Πίνακας 4.2 Ταξινόμηση στόχων και ικανοτήτων του αντιπάλου

Γενικά, αν και οι απαιτήσεις ασφάλειας μιας MAC συνάρτησης είναι παρόμοιες με αυτές των κρυπταλγόριθμων, υπάρχουν ορισμένες ουσιώδεις διαφορές. Πρώτον, στην περίπτωση των MAC ο σχεδιασμός των μονόδρομων συναρτήσεων έχει περισσότερους βαθμούς ελευθερίας, από τους κρυπταλγόριθμους. Στους κρυπταλγόριθμους η κρυπτογραφική πράξη θα πρέπει να είναι ενριπτική (injective), ώστε για κάθε κρυπτογράφηση να ορίζεται μοναδικά η αποκρυπτογράφηση. Στις MAC και γενικά στις μονόδρομες hash συναρτήσεις, η αντιστροφή δεν απαιτείται, οπότε οι υποψήφιες συναρτήσεις είναι πολύ περισσότερες.

Δεύτερον, μια συνάρτηση MAC προσφέρει αυθεντικοποίηση και όχι εμπιστευτικότητα. Για το λόγο αυτό δεν υπάρχουν νομικοί περιορισμοί στη χρήση της κρυπτογραφίας. Αντίθετα στην περίπτωση των κρυπταλγόριθμων όπου το μήνυμα κρυπτογραφείται, το μέγεθος του κλειδιού είναι νομικά ελεγχόμενο και εξαρτάται από τη χώρα στην οποία εκτελείται η κρυπτογράφηση. Στη Γαλλία για παράδειγμα είναι παράνομη η χρήση του κρυπταλγόριθμου Vigenère, όταν η κυβέρνηση δεν έχει αντίγραφο του κλειδιού. Ας θυμηθούμε ότι ο κρυπταλγόριθμος αυτός είναι μια απλή πρόσθεση modulo 2 του απλού κειμένου με κλειδί.

Από την πλευρά του αντιπάλου, αν και οι στόχοι και οι τρόποι επίθεσης των MAC έχουν ομοιότητες με αυτές των κρυπτοσυστημάτων, υπάρχουν βασικές διαφορές. Ανάλογα με την πληροφορία που μπορεί να έχει στην κατοχή του ο αντίπαλος, θα έχει και διάφορες ευκαιρίες επίθεσης. Στην περίπτωση ενός κρυπτοσυστήματος, θεωρούμε ότι ο αντίπαλος είτε προσπαθεί να βρει το κλειδί, είτε να αποκρυπτογραφήσει το κρυπτοκείμενο. Ανάλογα με τις δυνατότητες και ευκαιρίες που έχει ο αντίπαλος, υπάρχει το ενδεχόμενο να γνωρίζει ορισμένα ζευγάρια απλού κειμένου και κρυπτοκειμένου, οπότε στην περίπτωση αυτή μπορεί να εκτελέσει

την επίθεση με γνωστό απλό κείμενο. Αν όμως ο αντίπαλος δεν έχει πρόσβαση σε απλό κείμενο, τότε το σενάριο επίθεσης τον περιορίζει στην επίθεση γνωστού κρυπτοκειμένου. Στην περίπτωση των μονόδρομων hash συναρτήσεων, σε ένα μήνυμα του οποίου η αυθεντικοποίηση προστατεύεται με μια συνάρτηση MAC, ο αντίπαλος γνωρίζει πάντοτε το απλό κείμενο και την αντίστοιχη σύνοψη. Για να «σπάσει» την αυθεντικοποίηση, ο αντίπαλος θα πρέπει να ανακαλύψει το κλειδί της MAC.

Επομένως, η ασφάλεια της αυθεντικοποίησης εξαρτάται από το μήκος του κλειδιού. Αν θεωρήσουμε ότι η μόνη επίθεση που μπορεί να εκτελέσει κανείς στη MAC είναι η εξαντλητική αναζήτηση στο κλειδί, τότε μπορούμε να δείξουμε ότι η προσπάθεια που απαιτείται για να ανακαλύψει το κλειδί είναι ίση ή μεγαλύτερη από την προσπάθεια που θα έκανε για να ανακαλύψει το ίδιο (σε μέγεθος) κλειδί, σε ένα κρυπτοσύστημα. Για να είναι οι επιθέσεις στη MAC και στο κρυπτοσύστημα συγκρίσιμες, θεωρούμε ότι ο αντίπαλος έχει δυνατότητα επίθεσης γνωστού απλού κειμένου στο κρυπτοσύστημα, αφού στην περίπτωση της MAC παρέχεται μόνο αυθεντικοποίηση και όχι εμπιστευτικότητα.

Όπως γνωρίζουμε, στην επίθεση γνωστού κειμένου σε ένα κρυπτοσύστημα με κλειδί $\boldsymbol{k}$, ο αντίπαλος γνωρίζει ζεύγη απλού κειμένου και κρυπτοκειμένου p_i, c_i και επιλέγει συστηματικά κλειδιά $\boldsymbol{k}_j \in \boldsymbol{K}$, ώσπου να ανακαλύψει το κλειδί $\boldsymbol{k}$ για το οποίο $p_i = d_{\boldsymbol{k}}(c_i)$, ή ισοδύναμα $c_i = e_{\boldsymbol{k}}(p_i)$. Με εξαντλητική αναζήτηση, οι αναμενόμενες δοκιμές του αντιπάλου είναι $2^k/2$ ή 2^{k-1}, όπου k το μήκος του κλειδιού σε bits. Στην περίπτωση της επίθεσης στη MAC, εξετάζουμε δύο περιπτώσεις:

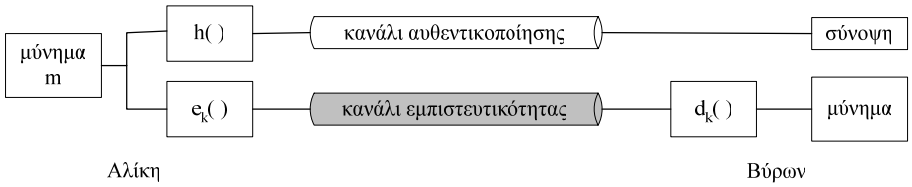
- $k > n$, το μήκος του κλειδιού είναι μεγαλύτερο από το μήκος της σύνοψης. Τότε για ένα ζευγάρι μηνύματος και σύνοψης, m_1, $h_{\boldsymbol{k}}(m_1)$, ο αντίπαλος θα πρέπει να ανακαλύψει το κλειδί $\boldsymbol{k}' \in \boldsymbol{K}$ για το οποίο $h_{\boldsymbol{k}'}(m) = h_{\boldsymbol{k}}(m)$. Αυτή όμως η ισότητα δεν εγγυάται ότι $\boldsymbol{k}' = \boldsymbol{k}$. Επειδή υπάρχουν περισσότερα κλειδιά από ότι συνόψεις, αναγκαστικά ορισμένα (διαφορετικά) κλειδιά θα αντιστοιχίζουν ένα μήνυμα στην ίδια σωστή σύνοψη. Μάλιστα ο αναμενόμενος αριθμός κλειδιών που θα παράγουν τη σωστή σύνοψη θα είναι ίσος με $2^k/2^n = 2^{k-n}$. Επομένως το ζητούμενο κλειδί βρίσκεται ανάμεσα στα 2^{k-n} κλειδιά που έχουν ξεχωρίσει. Για να μειωθεί το σύνολο αυτό, ο αντίπαλος θα πρέπει να επαναλάβει τη διαδικασία εξαντλητικής αναζήτησης με διαφορετικό ζευγάρι μηνύματος και σύνοψης m_2, $h_{\boldsymbol{k}}(m_2)$. Ο αναμενόμενος αριθμός σωστών κλειδιών σε αυτόν το δεύτερο γύρο θα είναι ίσος με $2^{k-n}/2^n = 2^{k-2n}$. Από την ποσότητα αυτή μπορούμε να συμπεράνουμε ότι οι αναμενόμενοι γύροι που πρέπει να πραγματοποιήσει ο αντίπαλος για να καταλήξει σε ένα μόνο κλειδί είναι k/n.
- $k \leq n$, το μήκος του κλειδιού είναι μικρότερο ή ίσο από το μήκος της σύνοψης. Στην περίπτωση αυτή, η πιθανότητα να αντιστοιχεί ένα μόνο κλειδί σε ένα ζευγάρι μηνύματος και σύνοψης, είναι μεγάλη. Αυτό είναι το οπτιμιστικό σενάριο για τον αντίπαλο, οπότε οι αναμενόμενες προσπάθειες που απαιτούνται για την ανακάλυψη του κλειδιού είναι 2^{k-1}. Το πεσιμιστι-

κό σενάριο είναι ότι περισσότερο από ένα κλειδιά μπορούν να παράγουν το δεδομένο ζευγάρι μηνύματος και σύνοψης, οπότε η προσπάθεια ακολουθεί την πρώτη περίπτωση.

Συμπεραίνουμε λοιπόν ότι στην καλύτερη περίπτωση ο αντίπαλος μπορεί να βρει το κλειδί που χρησιμοποιείται στη MAC με 2^{k-1} προσπάθειες. Επομένως η προσπάθεια ανάκτησης του κλειδιού σε μια συνάρτηση MAC είναι ίση ή μεγαλύτερη από την προσπάθεια αποκρυπτογράφησης μηνύματος που προέρχεται από κρυπτοσύστημα με κλειδί ίδιου μήκους.

Συνδυάζοντας αυθεντικοποίηση και εμπιστευτικότητα

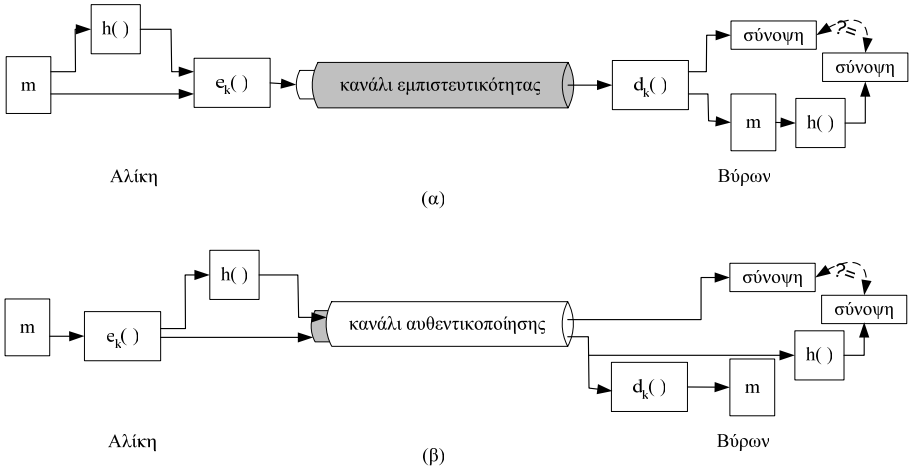
Στην πράξη για να πετύχουμε αυθεντικοποίηση και εμπιστευτικότητα χρειαζόμαστε από την κρυπτογραφία δύο συστατικά: μια κρυπτογραφική μονόδρομη hash και έναν κρυπταλγόριθμο. Η μονόδρομη hash δημιουργεί ένα κανάλι αυθεντικοποίησης, ενώ ο κρυπταλγόριθμος δημιουργεί ένα κανάλι εμπιστευτικότητας μεταξύ της Αλίκης και του Βύρωνα, όπως φαίνεται στο Σχήμα 4.7.



Σχήμα 4.7 Αυθεντικοποίηση και εμπιστευτικότητα

Ανάλογα με σειρά της εφαρμογής των δύο αυτών στοιχείων στο μήνυμα, έχουμε τις ακόλουθες περιπτώσεις:

- Αυθεντικοποίηση απλού κειμένου (Σχήμα 4.8α). Σύμφωνα με τη διάταξη αυτή, η αυθεντικοποίηση πραγματοποιείται στο απλό κείμενο. Έτσι η σύνοψη και το απλό κείμενο κρυπτογραφούνται από την e_k( ) και το κανάλι εμπιστευτικότητας περικλείει το κανάλι αυθεντικοποίησης, αφού πρέπει πρώτα να αποκρυπτογραφηθεί το μήνυμα και η σύνοψη, για να επακολουθήσει ο έλεγχος αυθεντικοποίησης. Η διάταξη της αυθεντικοποίησης του απλού κειμένου ονομάζεται και εσωτερικός έλεγχος σφαλμάτων.
- Αυθεντικοποίηση κρυπτοκειμένου (Σχήμα 4.8β). Η διάταξη αυτή παράγει τη σύνοψη του κρυπτοκειμένου, με αποτέλεσμα η εμπιστευτικότητα να προσφέρεται μόνο στο μήνυμα και όχι στη σύνοψη. Έτσι το κανάλι εμπιστευτικότητας βρίσκεται μέσα στο κανάλι αυθεντικοποίησης. Ο έλεγχος αυθεντικοποίησης πραγματοποιείται στο λαμβανόμενο κρυπτοκείμενο. Ο Βύρων ελέγχει πρώτα την αυθεντικότητα του κρυπτοκειμένου, και σε περίπτωση επιτυχούς αποτελέσματος ακολουθεί αποκρυπτογράφηση.



Σχήμα 4.8 Εναλλακτικές συνδυασμού αυθεντικοποίησης και εμπιστευτικότητας

Στα παραπάνω σενάρια υποθέσαμε ότι το κρυπτοσύστημα είναι συμμετρικό. Στην περίπτωση που χρησιμοποιείται ασύμμετρο κρυπτοσύστημα, εκτός από τις περιπτώσεις της αυθεντικοποίησης του απλού κειμένου και του κρυπτοκειμένου, έχουμε και την περίπτωση κρυπτογράφησης της σύνοψης με το ιδιωτικό κλειδί του αποστολέα.

ΟΡΙΣΜΟΣ 4.9 – Η διαδικασία η οποία ορίζεται από τη δημιουργία σύνοψης ενός μηνύματος και την κρυπτογράφηση αυτής με το ιδιωτικό κλειδί του αποστολέα, αποτελεί την ***ψηφιακή υπογραφή*** του μηνύματος.

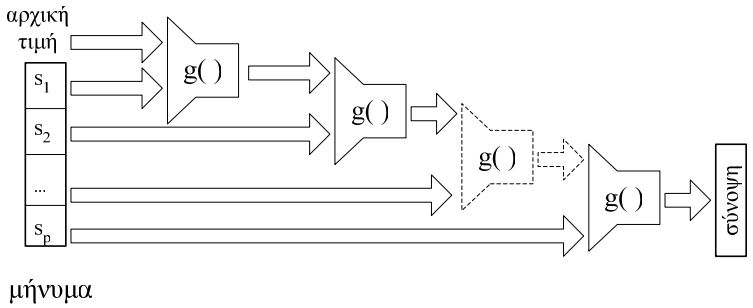
Η ψηφιακή υπογραφή αναφέρθηκε και στο Κεφάλαιο 1, όπου ο αποστολέας κρυπτογραφεί το απλό κείμενο με το ιδιωτικό του κλειδί. Στην πράξη η ψηφιακή υπογραφή εφαρμόζεται στη σύνοψη, για την αποφυγή της επίθεσης «αποκοπής-και-επικόλλησης» (cut-and-paste attack) που μπορεί να πραγματοποιηθεί σε πολλά ασύμμετρα κρυπτοσυστήματα. Αν θεωρήσουμε ότι ο ασύμμετρος κρυπταλγόριθμος εφαρμόζεται χωριστά σε τμήματα του μηνύματος, τότε η Αλίκη θα χρειαστεί να υπογράψει ψηφιακά ένα μήνυμα τόσες φορές, όσα είναι και τα τμήματα του μηνύματος. Το φυσικό ανάλογο είναι οι υπογραφές που μπαίνουν διαδοχικά στις σελίδες ενός συμβολαίου. Ωστόσο, η αδυναμία της πρακτικής αυτής είναι εντονότερη στον ψηφιακό κόσμο. Αν και θεωρητικά ο Βύρων μπορεί να πάρει σελίδες από διαφορετικά συμβόλαια τα οποία έχουν υπογραφεί από την Αλίκη σε διαφορετικές χρονικές στιγμές και να καταρτίσει ένα νέο συμβόλαιο, σε ένα ηλεκτρονικό μήνυμα τα τμήματα είναι πολύ μικρότερα. Ο Βύρων θα μπορούσε να απομονώσει προτάσεις ή ακόμη και λέξεις. Έτσι θα μπορούσε να κατασκευάσει ένα νέο συμβόλαιο έχοντας μεγάλη σχετικά ελευθερία κινήσεων, υπογεγραμμένο από την Αλίκη. Επομένως η πρακτική υπογραφής της σύνοψης είναι μια πολύ πιο ασφαλής λύση. Από πλευράς απαιτήσεων ασφάλειας της κρυπτογραφικής μονόδρομης hash

συνάρτησης, είναι ευνόητο ότι η συνάρτηση η οποία χρησιμοποιείται για την παραγωγή της σύνοψης προς υπογραφή θα πρέπει να έχει ασθενή ανθεκτικότητα σε συγκρούσεις. Απαιτείται να είναι υπολογιστικά αδύνατο για τον Βύρωνα να μπορεί να κατασκευάσει δεύτερο δικό του συμβόλαιο το οποίο να αντιστοιχίζεται στη σύνοψη του αρχικού συμβολαίου με την Αλίκη.

Η ψηφιακή υπογραφή θα μπορούσε να εφαρμοστεί τόσο στη σύνοψη του απλού κειμένου, όσο και στη σύνοψη του κρυπτογραφημένου κειμένου. Για δεοντολογικούς και πρακτικούς λόγους προτιμούμε η ψηφιακή υπογραφή να εφαρμόζεται στη σύνοψη του απλού κειμένου. Πρώτον, θα πρέπει να γνωρίζουμε που βάζουμε την υπογραφή μας. Υπογράφοντας ένα κρυπτοκείμενο δεν είναι δεοντολογικά ορθό. Δεύτερον, υπογράφοντας ένα κρυπτοκείμενο, ουσιαστικά υπογράφουμε τόσα απλά κείμενα όσα είναι και τα κλειδιά, επομένως παραβιάζεται η ίδια η υπόσταση της υπογραφής. Το φυσικό ανάλογο είναι η απάτη με το κρυφό καρμπόν που υπάρχει κάτω από μια σελίδα για να ξεγελάσουμε τον υπογράφοντα να υπογράψει παραπάνω από ένα κείμενα χωρίς τη συναίνεσή του.

Επαναληπτικές κρυπτογραφικές μονόδρομες hash συναρτήσεις

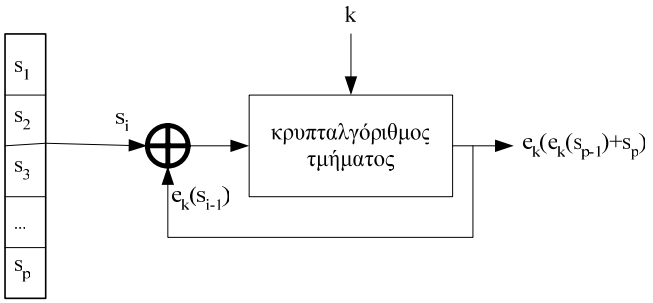
Οι μονόδρομες hash συναρτήσεις έχουν το χαρακτηριστικό να δέχονται για είσοδο μηνύματα που έχουν αυθαίρετο μήκος. Στην πράξη οι συναρτήσεις υλοποιούνται σε συστήματα με πεπερασμένες παραμέτρους όπως μνήμη, δίαυλο δεδομένων (data bus) και εντολών κτλ. Συνεπώς, η κατάτμηση του μηνύματος της εισόδου σε τμήματα και η επιμέρους επεξεργασία των τμημάτων αυτών είναι αναπόφευκτη. Έτσι, οι περισσότερες μονόδρομες συναρτήσεις βασίζονται στην επαναληπτική εφαρμογή μιας συνάρτησης $g : Z_2^m \to Z_2^n$ όπως φαίνεται στο Σχήμα 4.9. Η συνάρτηση g ονομάζεται ***συνάρτηση συμπίεσης*** και ο όρος αυτός καθώς και η αρχή της επαναληπτικής μονόδρομης οφείλονται στους Merkle και Damgard (1989). Αναλυτικότερα, σύμφωνα με τους Merkle και Damgard, αν η συνάρτηση συμπίεσης είναι ανθεκτική σε συγκρούσεις, τότε και η κατασκευή της επαναληπτικής μονόδρομης συνάρτησης θα είναι επίσης ανθεκτική σε συγκρούσεις.



Σχήμα 4.9 Επαναληπτική μονόδρομη hash.

Το κάθε τμήμα s_i του μηνύματος έχει μήκος *m*-*n* bits. Κατά την πρώτη εφαρμογή της *g*, τροφοδοτείται μια αρχική τιμή μήκους *n* bits και το τμήμα s_1. Η αρχική τιμή ονομάζεται ***διάνυσμα αρχικοποίησης*** (initialization vector) και χρησιμοποιείται για να συμπληρώσει το απαιτούμενο μήκος εισόδου των *m* bits. Στη δεύτερη εφαρμογή της *g* τροφοδοτούνται η έξοδος της *g* μαζί με το τμήμα s_2, κ.ο.κ. Η τελική σύνοψη προέρχεται από την αλυσίδα των επαναληπτικών εφαρμογών της *g* μέχρις ότου εξαντληθούν όλα τα τμήματα του μηνύματος.

Εναλλακτικά θα μπορούσαν να επιλεγούν όλα τα bits των ενδιάμεσων αποτελεσμάτων των *g*, όπως φαίνεται στο Σχήμα 4.10. Για επαναληπτική συνάρτηση χρησιμοποιείται κρυπταλγόριθμος τμήματος με *n* bits είσοδο και *n* bits έξοδο. Το ενδιάμεσο αποτέλεσμα προστίθεται στο επόμενο τμήμα του μηνύματος, ενώ η είσοδος του κλειδιού αποτελεί και το κλειδί της μονόδρομης hash.



Σχήμα 4.10 Επαναληπτική μονόδρομη hash βασισμένη σε κρυπταλγόριθμο τμήματος.

Ασφάλεια κρυπτογραφικών μονόδρομων hash

Υπάρχει μεγάλη ελευθερία τόσο στην επιλογή των κρυπτογραφικών μονόδρομων συναρτήσεων, όσο και στη συνδεσμολογία μεταξύ τους για τη δημιουργία άλλων μονόδρομων συναρτήσεων και αυτό φαίνεται από τον μεγάλο όγκο βιβλιογραφίας που ασχολείται ειδικά με τις συναρτήσεις αυτές. Ορισμένες κρυπτογραφικές μονόδρομες hash έχουν αντισταθεί όλες τις γνωστές επιθέσεις, ενώ πολλές φορές «ασήμαντες» μετατροπές και αλλαγές στη συνδεσμολογία τους δημιούργησαν συναρτήσεις οι οποίες μπορούσαν να σπάσουν με ευκολία. Ο βασικός στόχος του αντιπάλου είναι η δημιουργία συστηματικού τρόπου ανακάλυψης συγκρούσεων.

Έτσι, καταλήγουμε σε δύο κριτήρια τα οποία θα πρέπει να λαμβάνονται υπόψη στην κατασκευή ή επιλογή μιας κρυπτογραφικής μονόδρομης hash. Το πρώτο και βασικό κριτήριο αφορά κυρίως την επιλογή της συνάρτησης από την πληθώρα των διαθέσιμων συναρτήσεων που υπάρχουν στη βιβλιογραφία. Η υποψήφια συνάρτηση θα πρέπει να έχει αποδεδειγμένα αντισταθεί μέσα από τη βιβλιογραφία όλες τις γνωστές επιθέσεις και να έχει αναλυθεί επαρκώς. Νεοεμφανιζόμενες συναρτήσεις θα πρέπει να αντιμετωπίζονται με δυσπιστία ως προς την ασφάλειά τους.

Το δεύτερο κριτήριο αφορά την ανάλυση της υπόθεσης της εξαντλητικής αναζήτησης. Η επίθεση της εξαντλητικής αναζήτησης θα είναι πάντοτε παρούσα σε όλες τις πτυχές της κρυπτογραφίας. Επομένως, η σύγκριση της ασφάλειας της μονόδρομης συνάρτησης με την προσπάθεια της εξαντλητικής αναζήτησης είναι ένας τρόπος μέτρησης της κρυπτογραφικής της δύναμης. Μια κρυπτογραφική μονόδρομη συνάρτηση θεωρείται ασφαλής αν μπορεί να αντισταθεί σε επίθεση τουλάχιστον ίση με την εξαντλητική αναζήτηση.

ΠΑΡΑΔΕΙΓΜΑ 4.7 – Η εκθετική συνάρτηση ως μονόδρομη συνάρτηση. Θεωρούμε τη συνάρτηση $h(x)=a^x \bmod n$, με $1 < a < n$-1. Είναι γνωστό από τη θεωρία αριθμών (βλ. § 2.7- modular εκθετοποίηση) ότι για δοσμένο x, ο υπολογισμός του $a^x \bmod n$ είναι υπολογιστικά εύκολος, ενώ για δοσμένη $y = h(x)$, δεν υπάρχει αλγόριθμος ο οποίος να βρίσκει το αντίστοιχο x, με «ευκολία». Ο όρος «ευκολία» μεταφράζεται σε ποσοτική μέτρηση ως χαμηλές απαιτήσεις σε χρόνο ή (και) πόρους. Ένας μηχανικός για παράδειγμα, ορίζει τη μονόδρομη συνάρτηση ως τη συνάρτηση στην οποία απαιτούνται p λογικές πύλες όταν η είσοδος είναι το x και η έξοδος είναι το $h(x)$, και p^{ε} λογικές πύλες για να υπολογιστεί η έξοδος x από την είσοδο $h(x)$, όπου ε>1. Από πλευράς θεωρίας πολυπλοκότητας, ο ορισμός της ευκολίας του υπολογισμού δεν απέχει από την προσέγγιση του μηχανικού. Σύμφωνα με τη θεωρία πολυπλοκότητας, οι λογικές πύλες παραμετροποιούνται ως προς το χρόνο ή τις πράξεις που απαιτεί ο αλγόριθμος αντιστροφής της συνάρτησης. Για τον υπολογισμό της κανονικής φοράς της συνάρτησης, ο αλγόριθμος υπολογισμού έχει πολυπλοκότητα $O(\log_2 x)$.

Για τον υπολογισμό της αντίστροφης φοράς της συνάρτησης, ο οικονομικότερος αλγόριθμος είναι του Adleman, όπου απαιτούνται $e^{\sqrt{\ln n \cdot \ln(\ln n)}}$ στοιχειώδεις πράξεις. Αν και ο εκθέτης έχει αργό ρυθμό αύξησης, για μεγάλο n η εκθετική συνάρτηση παραμένει μονόδρομη. Ένας πιο κλασσικός αλγόριθμος είναι αυτός των Pohlig και Hellman με πολυπλοκότητα που εξαρτάται από το άθροισμα των παραγόντων του n-1.

Στη συνέχεια παραθέτουμε ορισμένες μονόδρομες hash συναρτήσεις οι οποίες θεωρούνται μέχρι σήμερα ασφαλείς.

MD4 και MD5

Η μονόδρομη hash MD4 και η διάδοχός της MD5 σχεδιάστηκαν από τον Rivest το 1990 και το 1992 αντίστοιχα. Λόγω της εύρεσης συγκρούσεων στην MD4 με 2^{20} υπολογισμούς, ήταν αναγκαία η αντικατάστασή της από την MD5. Όσον αφορά την MD5, δεν έχει καταγραφεί τρόπος εύρεσης συγκρούσεων. Προς το παρόν η μόνη αξιόλογη κριτική είναι το μικρό μήκος της σύνοψης που είναι 128 bits και υπάρχει το ενδεχόμενο επιτυχούς εξαντλητικής αναζήτησης.

Οι MD4 και MD5 μοιράζονται τους ίδιους στόχους ασφάλειας ο οποίοι είναι κατά Rivest (1990):

- **Ασφάλεια**. Θα πρέπει να είναι υπολογιστικά αδύνατο να βρεθούν δύο μηνύματα τα οποία να δίνουν το ίδιο αποτέλεσμα σύνοψης.
- **Άμεση ασφάλεια**. Ο αλγόριθμος δε θα βασίζεται σε υποθέσεις, όπως για παράδειγμα στη δυσκολία παραγοντοποίησης ακεραίων.
- **Ταχύτητα**. Ο αλγόριθμος θα είναι βασισμένος σε απλές λογικές πράξεις και ο σχεδιασμός του θα είναι βελτιστοποιημένος για 32-bit αρχιτεκτονικές υπολογιστών.
- **Απλότητα και κατάληψη μικρού χώρου**. Ο αλγόριθμος θα πρέπει να είναι σχετικά απλός στην περιγραφή του, χωρίς να απαιτεί μεγάλους πίνακες αντικατάστασης τιμών, ή μεγάλα σε μήκος προγράμματα.
- **Εύνοια αρχιτεκτονικής little-endian.** Η αρχιτεκτονική little-endian που είναι βασισμένοι οι επεξεργαστές της Intel x386, αποθηκεύουν το λιγότερα σημαντικό bit σε χαμηλή διεύθυνση μνήμης του byte, σε αντίθεση με την αρχιτεκτονική big-endian που είναι βασισμένοι οι επεξεργαστές Sparc. Έτσι ένας little-endian επεξεργαστής μπορεί να χρησιμοποιεί απ' ευθείας τις αποθηκευμένες δυαδικές λέξεις, ενώ στην περίπτωση του big-endian απαιτείται αντιστροφή. Επειδή γενικά οι big-endian επεξεργαστές είναι γρηγορότεροι στην εκτέλεση πράξεων, θεωρήθηκε ότι η προτίμηση έκφρασης του αλγόριθμου στη μορφή little endian εξισορροπεί τη διαφορά ταχύτητας μεταξύ των δύο οικογενειών επεξεργαστών.

Τεχνικά χαρακτηριστικά της MD5

Η MD5 δέχεται ως είσοδο ένα μήνυμα αυθαίρετου μήκους και παράγει σύνοψη μήκους 128 bits. Η επεξεργασία γίνεται σε τμήματα των 512 bits, όπου κάθε τμήμα συμμετέχει σε τέσσερις γύρους της συνάρτησης συμπίεσης.

Αρχικά στο μήνυμα προστίθενται bits ώστε το μέγεθός του να είναι ίσο με (448 mod 512). Το προστιθέμενο κομμάτι αποτελείται από μία μονάδα, συνοδευόμενη από τον απαιτούμενο αριθμό μηδενικών (1, 0, 0, …, 0). Το τελευταίο τμήμα του μηνύματος έχει μήκος 448 bits και τα υπόλοιπα 64 που μένουν για να συμπληρωθεί το μήκος των 512 bits χρησιμοποιείται για να αποθηκευθεί ο αριθμός που εκφράζει το συνολικό μήκος του μηνύματος mod 2^{64}. Τα 512 bits απαιτούν για την αποθήκευσή τους 16 δυαδικές λέξεις των 32 bit.

Οι ενδιάμεσες τιμές καθώς και το αποτέλεσμα της σύνοψης αποθηκεύονται σε 4 καταχωρητές A, B, C και D. Κατά την εκκίνηση της διαδικασίας οι καταχωρητές παίρνουν τις ακόλουθες αρχικές τιμές:

$A = (67452301)_{16}$
$B = (EFCDAB89)_{16}$
$C = (98BADCFE)_{16}$
$D = (19325476)_{16}$

Οι καταχωρητές αυτοί ονομάζονται ***αλυσιδωτές μεταβλητές*** (chaining variables). Η συνάρτηση συμπίεσης αποτελείται από τέσσερις γύρους και κάθε γύρος εκτελεί

16 πράξεις. Κάθε πράξη εκτελεί μία μη γραμμική συνάρτηση μεταξύ των τριών από τα A, B, C και D και προσθέτει το αποτέλεσμα στην τέταρτη μεταβλητή. Τέλος, το αποτέλεσμα αποθηκεύεται σε μια από τις αλυσιδωτές μεταβλητές.

Κάθε γύρος ορίζεται από μια πράξη η οποία εφαρμόζεται 16 φορές. Οι τέσσερις πράξεις είναι:

$$\underline{\text{Γύρος } j}:\ a \leftarrow b + ((a + R_j(b,c,d) + M_l + T[i]) <<< s) \mod 2^{32},\ \text{για } 1 \le j \le 4,$$

όπου:

a,b,c,d συνδυασμός των μεταβλητών A, B, C και D. Η σειρά και η αντιστοιχία μεταβάλλεται ανά γύρο και ανά πράξη,

M_l η l-στή δυαδική λέξη των 32 bit που αποτελεί το τμήμα των 512 bit

$T[i]$ κατά το i-στό βήμα, η τιμή που προκύπτει από το ακέραιο τμήμα της ποσότητας 2^{32} abs(sin(i)), με το i σε ακτίνια,

s η ποσότητα κυκλικής ολίσθησης του αποτελέσματος,

$R_j(\ )$, η μη γραμμική συνάρτηση του γύρου j. Οι τέσσερις μη γραμμικές συναρτήσεις είναι:

$$R_1(b,c,d) = bc + \bar{b}d$$
$$R_2(b,c,d) = bd + c\bar{d}$$
$$R_3(b,c,d) = b \oplus c \oplus d$$
$$R_4(b,c,d) = c \oplus (b + \bar{d})$$

Στο τέλος των τεσσάρων γύρων στις τελικές τιμές προστίθενται οι αρχικές τιμές των μεταβλητών A, B, C και D.

Secure Hash Algorithm, SHA

Η μονόδρομη συνάρτηση SHA δημοσιεύθηκε το 1993 από το Εθνικό Ινστιτούτο Τυποποίησης και Τεχνολογίας (NIST) και βασίζεται στον MD4, με τη διαφορά ότι η είσοδος δεν μπορεί να είναι μεγαλύτερη των 2^{64} bits. Επιπλέον, η σύνοψη έχει μέγεθος 160 bits έναντι της σύνοψης της MD4 που έχει μέγεθος 128 bits.

Η αρχική επεξεργασία του μηνύματος είναι ίδια με αυτήν της MD4, δηλαδή στο μήνυμα προστίθεται η ακολουθία (1, 0, 0, …, 0) έτσι ώστε το συνολικό μέγεθος να είναι ίσο με 448 mod 512. Στη συνέχεια, στα τελευταία 64 bits αποθηκεύεται το μέγεθος του μηνύματος.

Λόγω του μεγαλύτερου μήκους της σύνοψης χρησιμοποιούνται πέντε αλυσιδωτές μεταβλητές, έναντι των τεσσάρων που χρησιμοποιούνται στις MD4 και MD5. Οι μεταβλητές αυτές είναι οι A, B, C, D και E και οι αρχικές τιμές των τεσσάρων πρώτων μεταβλητών είναι όμοιες με αυτές της MD5, ενώ η πέμπτη μεταβλητή έχει την τιμή:

$E = (C3D2E1F0)_{16}$

Παρόμοια με την MD5, το κάθε τμήμα του μηνύματος υποβάλλεται σε τέσσερις γύρους, όπου ο κάθε γύρος αποτελείται από μια μη γραμμική πράξη που εφαρμόζεται 20 φορές. Οι τέσσερις πράξεις της SHA είναι οι ακόλουθες:

$$R_1(b,c,d) = bc + \bar{b}d$$

$$R_2(b,c,d) = b \oplus c \oplus d$$

$$R_3(b,c,d) = bc + bd + cd$$

$$R_4(b,c,d) = b \oplus c \oplus d$$

Μια άλλη διαφορά της SHA με την MD5 είναι μια επιπλέον συνάρτηση που επεκτείνει τα 512 bits του τμήματος του μηνύματος σε 2560 bits, ή ισοδύναμα σε 80 δυαδικές λέξεις των 32 bit. Έστω W_t, $0 \le t \le 79$ τα τμήματα που προκύπτουν από την επέκταση του τμήματος M_t. Η διαδικασία επέκτασης του M_t ορίζεται από:

$W_t = M_t$, για $0 \le t \le 15$, και

$W_t = (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) <<< 1$, για $16 \le t \le 79$.

Τέλος, ο κάθε γύρος είναι της μορφής:

Γύρος j: $(a,b,c,d,e) \leftarrow ((e + R_j(b,c,d) + S^5(A) + W_t + K_j), a, S^{30}(b), c, d)$,

όπου:

$S^k(a)$ η κυκλική ολίσθηση της μεταβλητής a κατά k bits,

t, ο αύξων αριθμός της πράξης ($0 \le t \le 79$),

K_j, μια από τις 4 σταθερές:

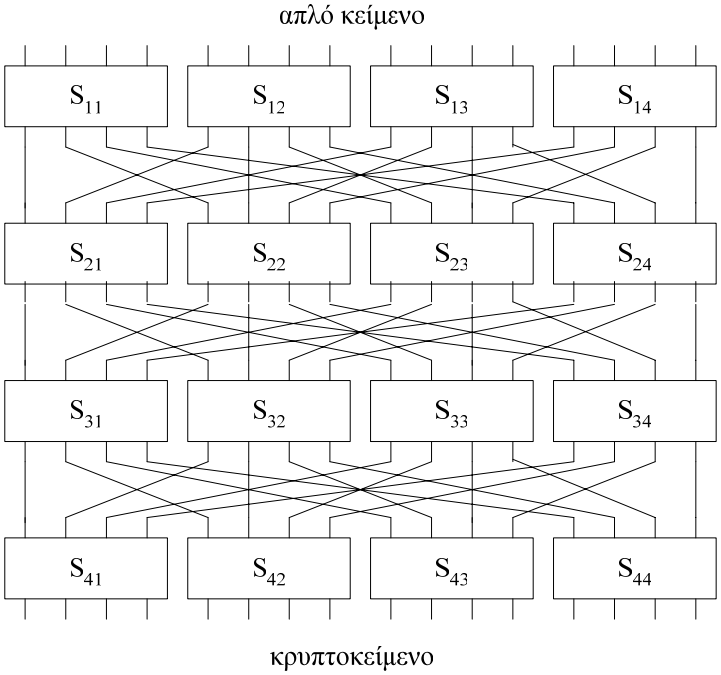
$K_1 = (5A827999)_{16}$
$K_2 = (6ED9EBA1)_{16}$
$K_3 = (8F1BBCDC)_{16}$
$K_4 = (CA62C1D6)_{16}$

4.4. Δίκτυα Αντικατάστασης-Μετάθεσης, ΔΑΜ

Τα Δίκτυα Αντικατάστασης-Μετάθεσης, ΔΑΜ (Substitution Permutation Networks, SPNs) βασίζονται στις αρχές του Shannon περί μετασχηματισμών ανάμειξης (mixing transformations), οι οποίες έχουν στόχο την υψηλή διάχυση και σύγχυση. Επάνω στις ιδέες του Shannon, οι Feistel et al. δημιούργησαν τα ΔΑΜ, όπου η διάχυση και η σύγχυση ελέγχεται από συγκεκριμένες συναρτήσεις. Πιο συγκεκριμένα, η υψηλή διάχυση επιτυγχάνεται από τα στάδια της μετάθεσης, ενώ η σύγχυση επιτυγχάνεται από τα στάδια της αντικατάστασης. Η αντικατάσταση υ-

λοποιείται με ***κουτιά αντικατάστασης*** (substitution boxes), τα οποία εισάγουν μη γραμμικότητα στην κατασκευή.

Ένας γύρος ορίζεται από μια σειρά κουτιών αντικατάστασης, συνοδευόμενο από μια συνάρτηση μετάθεσης. Οι παράμετροι που ορίζουν ένα ΔΑΜ είναι το μήκος της εισόδου n, ο αριθμός των γύρων r, και το μέγεθος των κουτιών αντικατάστασης $m \times m$. Στο Σχήμα 4.11 παρουσιάζεται ένα ΔΑΜ για $n = 16$, $r = 4$ και $m = 4$.



Σχήμα 4.11 ΔΑΜ με $n = 16$, $r = 4$ και $m = 4$ (Heys & Tavares, 1996).

4.4.1. Κουτιά αντικατάστασης

Συνήθως τα κουτιά αντικατάστασης είναι το μόνο μη γραμμικό βήμα σε έναν κρυπταλγόριθμο. Ένα κουτί αντικατάστασης αντιστοιχίζει m bits εισόδου σε n bits εξόδου. Για σχετικά μικρά κουτιά, η υλοποίησή τους πραγματοποιείται στις περισσότερες γλώσσες προγραμματισμού με ένα μονοδιάστατο πίνακα, όπου ο δείκτης του πίνακα είναι η είσοδος, ενώ το περιεχόμενο ορίζει την έξοδο.

ΠΑΡΑΔΕΙΓΜΑ 4.8 – Κουτί αντικατάστασης με μορφή πίνακα. Ο Πίνακας 4.3 παριστάνει ένα κουτί αντικατάστασης που αντιστοιχίζει δυαδικές λέξεις των 3 bit σε δυαδικές λέξεις των 4 bit.

Είσοδος i	$S(i)$	Είσοδος i	$S(i)$
000	1010	100	1111
001	1000	101	0010
010	0011	110	1110
011	0110	111	0010

Πίνακας 4.3 Κουτί αντικατάστασης $\{0,1\}^3 \rightarrow \{0,1\}^4$

Από πλευράς κρυπτογραφίας, οι παράμετροι που παρουσιάζουν ενδιαφέρον είναι το μέγεθος του κουτιού και φυσικά ο τρόπος συμπλήρωσης των «μαγικών» αριθμών του περιεχομένου του. Ο ορθόδοξος τρόπος σχεδιασμού ενός κουτιού αντικατάστασης είναι να τεθούν τα κριτήρια αξιολόγησης και να επιλεγούν οι δύο παράμετροι ώστε να πληρούνται τα κριτήρια αυτά. Οι Adams και Tavares έθεσαν τα ακόλουθα κριτήρια τα οποία πρέπει να πληροί ένα κουτί αντικατάστασης για να είναι κρυπτογραφικώς επιθυμητό:

- **Μη γραμμικότητα**. Αυτό είναι το πιο σημαντικό κριτήριο γιατί η ασφάλεια ενός κρυπτοσυστήματος είναι άρρηκτα συνδεδεμένη με τη μη γραμμικότητα. Ένα κουτί αντικατάστασης το οποίο είναι γραμμικό, μπορεί να κρυπταναλυθεί με μεγάλη ευκολία. Στο επόμενο κεφάλαιο θα παρουσιάσουμε τη μέθοδο της γραμμικής κρυπτανάλυσης η οποία επιδιώκει να προσεγγίσει τα κουτιά αντικατάστασης με γραμμικές σχέσεις.
- **Αμφίεση** (bijection).Το κριτήριο αυτό είναι απαραίτητο για να ορίζεται μονοσήμαντα η αποκρυπτογράφηση. Έτσι στο σχεδιασμό μονόδρομων συναρτήσεων hash, το κριτήριο αυτό δεν είναι απαραίτητο. Επίσης σε πολλά κρυπτοσυστήματα, το κουτί αντικατάστασης μπορεί να συμμετέχει με τρόπο τέτοιο ώστε να ορίζεται η αποκρυπτογράφηση, ενώ το κουτί αντικατάστασης να μην είναι αμφιενριπτικό (bijective). Ένα παράδειγμα κρυπτοσυστήματος όπου δεν απαιτεί αμφιενριπτικά κουτιά αντικατάστασης είναι τα δίκτυα Feistel, που εξετάζονται στην επόμενη ενότητα.
- **Αυστηρή χιονοστιβάδα**. Το «κριτήριο της αυστηρής χιονοστιβάδας» (strict avalanche criterion), οφείλεται στους Webster και Tavares και συσχετίζεται με τα χαρακτηριστικά της σύγχυσης και διάχυσης του Shannon (Κεφ. 3). Ένα κουτί αντικατάστασης πληροί το κριτήριο της αυστηρούς χιονοστιβάδας, όταν για οποιοδήποτε bit εισόδου η αντιστροφή του έχει τη δυνατότητα να προκαλέσει αντιστροφή οποιουδήποτε bit της εξόδου, με πιθανότητα 0,5.
- **Ανεξαρτησία των bits της εξόδου**. Θα πρέπει το κουτί αντικατάστασης να μην εμφανίζει σχέσεις μεταξύ των bits της εξόδου. Μια σχέση για παράδειγμα είναι: «το bit i είναι η αντιστροφή του bit j, με πιθανότητα 0,9». Η ύπαρξη αυτοσυσχέτισης δύο ή περισσοτέρων bits της εξόδου μειώνει το χώρο αναζήτησης.

Από τα παραπάνω κριτήρια, το πιο καίριο από πλευράς ασφάλειας είναι η μη γραμμικότητα. Ο σχεδιασμός κουτιών αντικατάστασης με υψηλή μη γραμμικότητα περιλαμβάνει μελέτη μιας κατηγορίας Μπουλιανών συναρτήσεων που ονομάζονται ***κεκαμμένες*** (bent). Οι κυρτές συναρτήσεις μπορούν να παράγουν κουτιά αντικατάστασης τα οποία πληρούν το κριτήριο της μη γραμμικότητας.

Μια εναλλακτική προσέγγιση κατασκευής των κουτιών αντικατάστασης είναι η συμπλήρωση των περιεχομένων τους με τυχαίες τιμές. Έχει δειχθεί ότι η μέθοδος αυτή για σχετικά μικρά κουτιά αντικατάστασης είναι ανασφαλής. Τα κουτιά που ορίζονται στους περισσότερους κρυπταλγόριθμους τμήματος θεωρούνται μικρά και η έρευνα έχει δείξει ότι αν τα κουτιά αντικατασταθούν με κουτιά των οποίων οι τιμές είναι τυχαίες, το κρυπτοσύστημα που προκύπτει είναι αρκετές τάξεις μεγέθους πιο αδύναμο. Το συμπέρασμα λοιπόν είναι ότι για μικρά κουτιά αντικατάστασης, τα περιεχόμενα θα πρέπει να προκύπτουν από μεθόδους οι οποίες να εγγυώνται μη γραμμικότητα, ενώ στην περίπτωση των μεγάλων κουτιών αντικατάστασης, η συμπλήρωση με τυχαίες τιμές μπορεί να συντηρήσει τη μη γραμμικότητα.

Όσον αφορά το μέγεθος των κουτιών αντικατάστασης, το μέγεθος m της εισόδου σε σχέση με το μέγεθος n της εξόδου καθορίζουν τα περιθώρια ύπαρξης γραμμικών σχέσεων. Αν $n \geq 2^m$-m, τότε θα υπάρχει γραμμική σχέση μεταξύ των bits της εξόδου με την είσοδο, οπότε και το κουτί αντικατάστασης δε θα μπορεί να αντισταθεί σε γραμμική κρυπτανάλυση. Στην περίπτωση που $m \geq 2^n$, τότε θα υπάρχουν γραμμικές σχέσεις μεταξύ των bits της εξόδου, γεγονός που μειώνει το χώρο αναζήτησης.

4.4.2. Δίκτυα Αντικατάστασης-Μετάθεσης με κλειδί

Όταν τα κουτιά αντικατάστασης είναι αμφιενριπτικά και το μέγεθος της εξόδου είναι ίσο με αυτό της εισόδου ($m = n$), τότε τα κουτιά αυτά ορίζουν μεταθέσεις στο σύνολο $\{0, 1\}^n$. Τα κρυπτοσυστήματα που μπορούν να περιγραφούν ως μεταθέσεις έχουν διερευνηθεί σε μεγάλο βαθμό, καθώς οι περισσότεροι σύγχρονοι κρυπταλγόριθμοι τμήματος περιλαμβάνονται στην κατηγορία των συναρτήσεων που είναι μεταθέσεις.

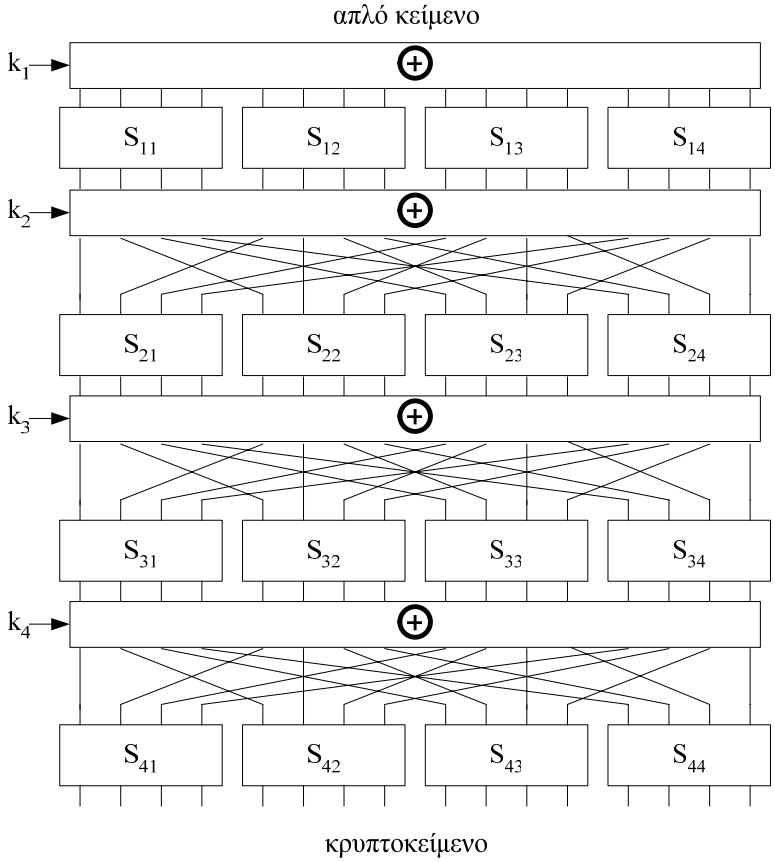
ΟΡΙΣΜΟΣ 4.10 – Έστω οι κρυπτογραφικές πράξεις e_s: $\{0, 1\}^m \rightarrow \{0, 1\}^m$ (αντικατάσταση) και e_p:$\{1, 2, \ldots, n\} \rightarrow \{1,2,\ldots,n\}$ (αναδιάταξη), με $(n/m) \in \boldsymbol{Z}$. Το κρυπτοσύστημα δικτύου αντικατάστασης-μετάθεσης είναι ένα κρυπτοσύστημα γινομένου $\boldsymbol{\mathcal{F}} = \boldsymbol{\mathcal{G}} = \boldsymbol{K} = \{0, 1\}^n$, με $e \in \boldsymbol{E}$ και $d \in \boldsymbol{D}$ και πρόγραμμα κλειδιού $\{\mathbf{k}_1,\mathbf{k}_{2,\ldots,}\mathbf{k}_r\}$, τέτοια ώστε:

$$e_{\{\mathbf{k}_1,\mathbf{k}_2,\ldots,\mathbf{k}_r\}}(\mathbf{p}) = e_p(e_s(\mathbf{k}_r \oplus e_p(e_s(\mathbf{k}_{r-1} \oplus \ldots \oplus e_p(e_s(\mathbf{k}_1 \oplus \mathbf{p})\ldots)) \text{ και}$$

$$d_{\{\mathbf{k}_1,\mathbf{k}_2,\ldots,\mathbf{k}_r\}}(\mathbf{c}) = e_s^{-1}(\mathbf{k}_1 \oplus e_p^{-1}(e_s^{-1}(\mathbf{k}_2 \oplus \ldots \oplus e_p^{-1}(e_s^{-1}(\mathbf{k}_r \oplus e_p^{-1}(\mathbf{c}))\ldots)).$$

Από τον παραπάνω ορισμό προκύπτει ότι το μέγεθος των κουτιών αντικατάστασης θα είναι $m \times m$, οπότε σε κάθε γύρο θα χρησιμοποιούνται n/m κουτιά. Το κρυπτοσύστημα αποτελείται από r γύρους, επομένως στο κρυπτοσύστημα εκτελούνται $2r$-1 κρυπτογραφικά γινόμενα (οι δύο πράξεις αντιστοιχούν σε ένα γινόμενο, οι τρεις σε δύο, οι τέσσερις σε τρεις, κοκ).

Από το ΔΑΜ του Σχήματος 4.11 με $n = 16$, $r = 4$ και $m = 4$, προκύπτει το κρυπτοσύστημα ΔΑΜ όπως φαίνεται στο Σχήμα 4.12. Σύμφωνα με τον Ορισμό 4.10, όλα τα κουτιά αντικατάστασης είναι τα ίδια. Μια δημοφιλής παραλλαγή η οποία συναντάται σε πολλά κρυπτοσυστήματα που περιλαμβάνουν στάδιο από κουτιά αντικατάστασης, είναι τα κουτιά να είναι διαφορετικά. Έτσι στο ΔΑΜ του σχήματος θα υπάρχουν 4 διαφορετικά κουτιά αντικατάστασης τα οποία επαναλαμβάνονται 4 φορές. Το κάθε κουτί εμφανίζεται μια φορά στον κάθε γύρο, δηλαδή $S_{1i} = S_{2i} = S_{3i} = S_{4i}$, για $1 \le i \le 4$.



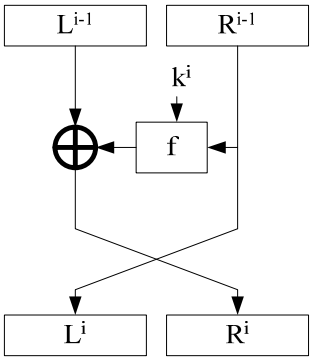
Σχήμα 4.12 Κρυπτοσύστημα ΔΑΜ

Προαιρετικά, στο τέλος του τελευταίου γύρου κατά την κρυπτογράφηση, το κρυπτοκείμενο μπορεί να συνδυαστεί με μια πρόσθετη ποσότητα κλειδιού $\mathbf{k}_{r+1}$, με αποκλειστική διάζευξη. Η διαδικασία όπου η κρυπτογράφηση και αποκρυπτογράφηση περικλείονται με αποκλειστική διάζευξη των εισόδων και εξόδων με κλειδιά, ονομάζεται ***λεύκανση*** (whitening). Η λεύκανση είναι ένας αποτελεσματικός τρόπος πρόληψης εφαρμογής της κρυπτανάλυσης, εφόσον τα κλειδιά δεν είναι γνωστά. Λόγω της ιδιότητας που έχει η αποκλειστική διάζευξη να ακυρώνει την ποσότητα που εφαρμόζεται δύο φορές διαδοχικά, το κλειδί του κάθε γύρου απομακρύνεται με ευκολία κατά τη διαδικασία αποκρυπτογράφησης.

Ωστόσο, η λεύκανση κρύβει και κινδύνους. Λόγω της μεγαλύτερης έκθεσης των κλειδιών στον αντίπαλο, αν το κρυπτοκείμενο ή το απλό κείμενο γίνουν γνωστά, τότε ο αντίπαλος μπορεί να ανακαλύψει τα κλειδιά λεύκανσης της εξόδου ή της εισόδου αντίστοιχα. Επειδή όμως τα κλειδιά προκύπτουν από ένα αρχικό κλειδί μέσω της γεννήτριας προγράμματος κλειδιών, η ασφάλεια του κρυπτοσυστήματος μεταφέρεται στη διαδικασία δημιουργίας του προγράμματος των κλειδιών. Επομένως, ο αντίπαλος έχοντας στην κατοχή του ένα (ή και περισσότερα) από τα κλειδιά, θα επιχειρήσει επίθεση στη συνάρτηση της γεννήτριας. Η ασφάλεια των γεννητριών του προγράμματος κλειδιών εξετάζεται στο Κεφάλαιο 3.

4.5. Δίκτυα Feistel

Η κρυπτογραφική πράξη τύπου Feistel είναι της μορφής του Σχήματος 4.13, η οποία αποτελεί και έναν γύρο σε κρυπτοσύστημα γινομένου. Το βασικό χαρακτηριστικό ενός δικτύου Feistel είναι η πλήρης ελευθερία στην επιλογή της ***συνάρτησης γύρου*** *f*. Η δομή του δικτύου Feistel είναι τέτοια ώστε η αντίστροφη σχέση ορίζεται πάντοτε, ακόμα και αν η συνάρτηση *f* δεν είναι ενριπτική. Επιπλέον, σε ορισμένες περιπτώσεις ένα δίκτυο Feistel μπορεί να είναι αποδείξιμα ασφαλές, όπως θα δείξουμε παρακάτω.



Σχήμα 4.13 Ένας γύρος Feistel

Σε κάθε γύρο η είσοδος χωρίζεται στο αριστερό και στο δεξιό τμήμα. Τα δύο τμήματα της εισόδου του *i*-στού γύρου συμβολίζονται με L^{i-1} και R^{i-1}, ενώ οι έξο-

δοι συμβολίζονται με L^i και R^i. Στον πρώτο γύρο τα τμήματα L^0 και R^0 αντιστοιχούν στο απλό κείμενο, ενώ στον τελικό γύρο, τα τμήματα L^r και R^r αντιστοιχούν στο κρυπτοκείμενο.

Κατά τον γύρο *i*, η συνάρτηση γύρου f δέχεται ως είσοδο το δεξιό τμήμα της εισόδου και το κλειδί k^i το οποίο προέρχεται από το πρόγραμμα κλειδιού. Η έξοδος της συνάρτησης συνδυάζεται με το αριστερό τμήμα της εισόδου με αποκλειστική διάζευξη και το αποτέλεσμα της πράξης αντιστοιχίζεται στο δεξιό τμήμα της εξόδου, ενώ το δεξιό τμήμα της εισόδου αντιστοιχίζεται στο αριστερό τμήμα της εξόδου. Η ανταλλαγή του αριστερού τμήματος με το δεξί έχει ως αποτέλεσμα ο επόμενος γύρος να εφαρμόσει το αποτέλεσμα της συνάρτησης σε εκείνο το τμήμα της εισόδου το οποίο μεταφέρθηκε ατόφιο από την είσοδο στην έξοδο. Είναι φανερό ότι σε κρυπτοσύστημα με έναν και μόνο γύρο, το δεξιό τμήμα του κρυπτοκειμένου θα είναι ίσο με το αριστερό τμήμα του απλού κειμένου. Αυτό είναι ένα χαρακτηριστικό της κρυπτογραφικής πράξης τύπου Feistel και θεωρητικά ένα δίκτυο όπου τα δύο τμήματα εισόδου έχουν το ίδιο μέγεθος, θα πρέπει να περιλαμβάνει τουλάχιστον τρεις γύρους προκειμένου το κρυπτοσύστημα να έχει τη δυνατότητα να αποκρύψει πλήρως το απλό κείμενο. Στην πράξη όμως απαιτούνται πολύ περισσότεροι γύροι για να είναι ένα κρυπτοσύστημα τύπου Feistel ασφαλές. Ο αριθμός των γύρων καθώς και η κρυπτογραφική δύναμη του κρυπτοσυστήματος εξαρτάται από τη συνάρτηση *f*.

Έστω n_L και n_R το μέγεθος σε bits του αριστερού και δεξιού τμήματος αντίστοιχα, με συνολικό μήκος εισόδου $n = n_L + n_R$. Η συνάρτηση γύρου θα ορίζει την αντιστοιχία $f : \{0,1\}^{n_R} \rightarrow \{0,1\}^{n_L}$. Αν $n_L = n_R = n/2$, το δίκτυο Feistel ονομάζεται ***ισορροπημένο***. Η πράξη κρυπτογράφησης ορίζεται από την επανάληψη της κρυπτογραφικής πράξης:

$$e^i_{k^i}(L^i, R^i) = L^{i-1} \,||\, (f(R^{i-1}, k^i) \oplus L^{i-1}), \quad \text{για } 0 < i \leq r,$$

όπου $a||b$ το δυαδικό τμήμα το οποίο αποτελείται από την αλληλουχία των τμημάτων *a* και *b*. Για το απλό κείμενο θα είναι $\mathbf{p} = L^0||R^0$, ενώ για το κρυπτοκείμενο θα είναι $\mathbf{c} = L^r||R^r$. Το κλειδί επιλέγεται σε κάθε γύρο από το πρόγραμμα κλειδιού $\{k^1, k^2, \ldots, k^r\}$. Κατά την αποκρυπτογράφηση εφαρμόζεται η ίδια πράξη, με τη διαφορά ότι το πρόγραμμα κλειδιού ακολουθεί την αντίστροφη σειρά, $\{k^r, k^{r-1}, \ldots, k^1\}$.

Το τμήμα της εισόδου το οποίο τροφοδοτείται στη συνάρτηση γύρου ονομάζεται ***προέλευση***, ενώ το τμήμα της εισόδου στο οποίο εφαρμόζεται το αποτέλεσμα της συνάρτησης με αποκλειστική διάζευξη ονομάζεται ***στόχος***. Αν το μέγεθος της πηγής είναι μεγαλύτερο από το μέγεθος του στόχου, τότε το δίκτυο ονομάζεται ***δίκτυο Feistel σημαίνουσας προέλευσης***, ενώ στην περίπτωση που το μέγεθος του στόχου είναι μεγαλύτερο, το δίκτυο ονομάζεται ***δίκτυο Feistel σημαίνοντος στόχου***. Αν το άθροισμα του μεγέθους της πηγής και του στόχου είναι ίσο με το μέγεθος της εισόδου, τότε το δίκτυο ονομάζεται ***τέλειο***, ενώ στην περίπτωση που το άθροισμα της πηγής και του στόχου είναι μικρότερο, το δίκτυο ονομάζεται ***ατελές***. Σε ένα ατελές δίκτυο υπάρχει τμήμα της εισόδου το οποίο εμφανίζεται ατόφιο στη

έξοδο και επιπλέον δεν συμπεριλαμβάνεται στην πράξη της συνάρτησης γύρου. Το τμήμα αυτό ονομάζεται ***μηδενικό***.

Στη βιβλιογραφία το συντριπτικό ποσοστό στην έρευνα των δικτύων Feistel αποδίδεται σε ισορροπημένα δίκτυα Feistel, δηλαδή το αριστερό τμήμα της εισόδου είναι ο στόχος και είναι ίσο με το δεξιό τμήμα της εισόδου που είναι η προέλευση. Ο βασικός λόγος εκτενούς μελέτης των ισορροπημένων δικτύων Feistel είναι επειδή τα πιο διαδεδομένα κρυπτοσυστήματα τα οποία βασίζονται σε δίκτυα Feistel είναι ισορροπημένα, όπως το κρυπτοσύστημα DES που μελετάμε στο επόμενο κεφάλαιο. Ωστόσο, η ασύμμετρη κατανομή των τμημάτων της εισόδου σε δίκτυα Feistel σημαίνουσας προέλευσης και σημαίνοντος στόχου δημιουργεί υποψίες ότι ένα μη ισορροπημένο δίκτυο Feistel μπορεί να είναι κρυπτογραφικά αδύναμο. Στην περίπτωση του δικτύου Feistel σημαίνοντος στόχου θα υπάρχουν σε κάθε γύρο γραμμικές σχέσεις μεταξύ ορισμένων bits εισόδου με ορισμένα bits εξόδου. Στην περίπτωση δικτύου Feistel σημαίνουσας προέλευσης θα απαιτούνται περισσότεροι γύροι για να εμφανισθεί κάθε bit στο τμήμα του στόχου.

4.5.1. Ασφάλεια δικτύων Feistel

Η μελέτη και τεκμηρίωση της ασφάλειας των δικτύων Feistel είναι μια από τις πιο χαρακτηριστικές περιπτώσεις της σύγχρονης κρυπτογραφίας. Η προσέγγιση σε ένα αποδείξιμα ασφαλές κρυπτοσύστημα ακολουθεί τα εξής βασικά στάδια:

1. Αναγνώριση του προβλήματος, όπου ξεχωρίζουμε ένα πρόβλημα κρυπτογραφίας. Ένα από τα κλασσικά προβλήματα, για παράδειγμα, είναι: «Η f είναι μονόδρομη συνάρτηση;»
2. Καθορισμός του προβλήματος. Αυτό είναι ίσως το πιο βασικό στάδιο στο οποίο περιγράφουμε μαθηματικά το πρόβλημα.
3. Ανάπτυξη του πρωτοκόλλου το οποίο καθορίζει τα βήματα τα οποία θα ακολουθήσουμε για να αποδείξουμε την ασφάλεια του προβλήματος.
4. Καθορισμός της υποθέσεως, η οποία αναφέρεται στις δυνατότητες του αντιπάλου.
5. Απόδειξη. Με βάση την υπόθεση, εκτελούμε το πρωτόκολλο για να προσδιορίσουμε αν το πρόβλημα το οποίο έχουμε καθορίσει οδηγεί σε ασφαλή κατασκευή.

Θα χρησιμοποιήσουμε την παραπάνω μεθοδολογία για να κατασκευάσουμε ένα δίκτυο Feistel το οποίο θα είναι αποδείξιμα ασφαλές. Ο τρόπος προσέγγισης του προβλήματος που θα ακολουθήσει είναι βασισμένος σε εργασίες αξιόλογων ερευνητών (Goldreich, Goldwasser, Micali, Luby, Rackoff, Rogaway), των οποίων η συμβολή στη σύγχρονη κρυπτογραφία ήταν καθοριστική.

Μεταθέσεις, αντίπαλοι και μαντεία

Με μια πρώτη ματιά ο τίτλος της ενότητας αυτής ίσως δημιουργεί περισσότερες απορίες παρά απαντήσεις. Ο καθορισμός των τριών αυτών συστατικών θέτει το

τοπίο στο οποίο τα συστατικά αυτά θα αλληλεπιδράσουν μεταξύ τους, προκειμένου να φτάσουμε στην απόδειξη του ασφαλούς κρυπτοσυστήματος.

Θεωρούμε το σύνολο $S^n = \{0, 1\}^n$. Το σύνολο αυτό αποτελείται από δυαδικές λέξεις μήκους n. Το πλήθος των στοιχείων του συνόλου S^n είναι $|S^n| = 2^n$. Έστω τώρα το σύνολο F^n το οποίο αποτελείται από όλες τις δυνατές συναρτήσεις που αντιστοιχίζουν το S^n στον εαυτό του, δηλαδή:

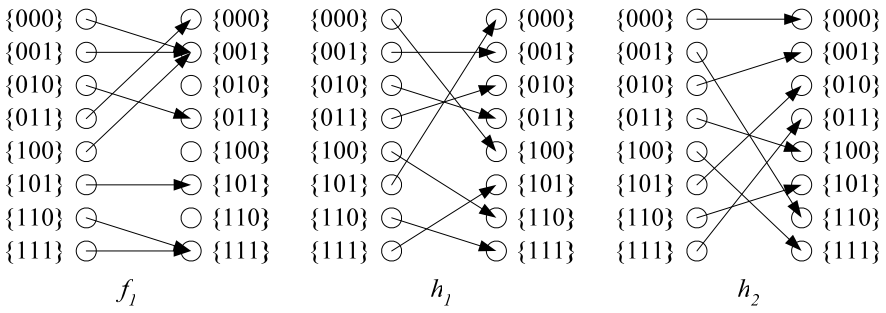
$$f \in F^n, f : \{0,1\}^n \to \{0,1\}^n$$

Το πλήθος όλων των δυνατών αντιστοιχίσεων θα είναι ίσο με:

$$| F^n | = | S^n |^{2^n} = 2^{n2^n} .$$

Έστω ότι από τις αντιστοιχίσεις του F^n «φιλτράρουμε» αυτές οι οποίες είναι αντιστρέψιμες, δηλαδή 1-1 και επί (αμφιέσεις), και έστω P^n το σύνολο αυτών. Τότε το P^n θα αποτελείται από συναρτήσεις οι οποίες είναι ***μεταθέσεις*** των στοιχείων του συνόλου S^n.

ΠΑΡΑΔΕΙΓΜΑ 4.9 – Στο Σχήμα 4.14 φαίνονται μια αντιστοίχιση f_1 και δύο μεταθέσεις $h_1, h_2 \in P^3$, του συνόλου $S^3 = \{000,001,010,011,100,101,110,111\}$.



Σχήμα 4.14 Παραδείγματα αντιστοίχισης και μεταθέσεων του S^3

Είναι φανερό από το παραπάνω σχήμα ότι οι μεταθέσεις h_1, h_2 είναι αντιστρέψιμες, ενώ η αντιστοίχιση f_1 δεν είναι.

Το πλήθος των στοιχείων του συνόλου των μεταθέσεων P^n είναι $|P^n| = (2^n!)$. Ο αριθμός αυτός είναι κατά πολύ μικρότερος του πλήθους όλων των δυνατών αντιστοιχίσεων που ανήκουν στο σύνολο F^n.

Γνωρίζοντας επομένως το πλήθος των μεταθέσεων, μπορούμε να τις απαριθμήσουμε:

$$P^n = \{h_1, h_2, ..., h_{2^n!}\} .$$

Έχοντας προσδιορίσει πλήρως το σύνολο των μεταθέσεων, μπορούμε να κατασκευάσουμε ένα κρυπτοσύστημα όπου το απλό κείμενο και το κρυπτοκείμενο αποτελείται από στοιχεία του S^n, και το κλειδί k θα είναι ο δείκτης της μετάθεσης, δηλαδή $h_k \in P^n$. Αν το κλειδί εκφράζεται με δυαδική λέξη, τότε για να μπορέσει το κρυπτοσύστημα να περιλάβει όλες τις μεταθέσεις, το μέγεθος του κλειδιού θα πρέπει να είναι ίσο με $\log_2(2^n!)$. Στην πράξη όμως το κλειδί είναι κατά πολύ μικρότερο. Μάλιστα, δεν θα θέλαμε το κρυπτοσύστημα να μπορεί να διατρέξει όλες τις δυνατές μεταθέσεις, γιατί μέσα σε αυτές υπάρχουν και οι μεταθέσεις όπως $h_i(p)=c$, όπου το κρυπτοκείμενο είναι ίσο με το απλό κείμενο. Γενικότερα, υπάρχουν μεταθέσεις οι οποίες δεν καταλήγουν σε ασφαλή κρυπτογράφηση. Επομένως τίθεται το ερώτημα για το ποιες από τις μεταθέσεις απαρτίζουν ένα ασφαλές κρυπτοσύστημα.

Σε αυτό το σημείο εισάγεται η έννοια του ***αντιπάλου***. Ως αντίπαλο θεωρούμε ένα πρόγραμμα το οποίο έχει τον ακόλουθο σκοπό (Luby και Rackoff):

«Έστω δύο μαύρα κουτιά για τα οποία τα μόνα στοιχεία που έχει ο αντίπαλος είναι ότι το ένα από αυτά υπολογίζει σταθερά μια συγκεκριμένη συνάρτηση από το F^n και το άλλο υπολογίζει μια συνάρτηση h_k για σταθερό k και άγνωστο προς τον αντίπαλο. Το κρυπτοσύστημα είναι ασφαλές, αν ο αντίπαλος δεν είναι σε θέση να διακρίνει μέσα σε «λογικά» όρια χρόνου και «λογικό» αριθμό ερωτήσεων, πιο από τα μαύρα κουτιά περιέχει την μετάθεση και πιο την απλή αντιστοίχιση».

Η παραπάνω πρόταση περιέχει κάποιες έννοιες που θα πρέπει να καθοριστούν με περισσότερη σαφήνεια και ακρίβεια. Για τον λόγο αυτό ορίζουμε την έννοια του ***πλεονεκτήματος*** του αντιπάλου. Έστω ότι ο αντίπαλος Α τροφοδοτείται είτε με τα αποτελέσματα από τη μετάθεση, είτε με αποτελέσματα από την συνάρτηση αντιστοίχισης. Υποθέτουμε ότι ο αντίπαλος απαντάει με **0** αν πιστεύει ότι τα αποτελέσματα που λαμβάνει δεν προέρχονται από την εφαρμογή της μετάθεσης, ενώ απαντάει με **1** αν πιστεύει ότι τα αποτελέσματα προέρχονται από τη συνάρτηση μετάθεσης. Τότε μπορούμε να ορίσουμε ποσοτικά το πλεονέκτημα δ του αντιπάλου ως:

$$\delta(A) = \Pr\{A(f) = 1 : f \in H^n\} - \Pr\{A(f) = 1 : f \in F^n\}$$

όπου $H^n \subset P^n$, το σύνολο που αποτελείται από τις επιτρεπόμενες μεταθέσεις του κρυπτοσυστήματος. Το σύνολο των μεταθέσεων H^n που ορίζεται από ένα κρυπτοσύστημα είναι στην πράξη κατά πολύ μικρότερο από το σύνολο όλων των μεταθέσεων P^n και αυτό οφείλεται στο σχετικά μικρό μέγεθος του κλειδιού. Όσον αφορά το πλεονέκτημα, για τιμές κοντά στο μηδέν, σημαίνει ότι ο αντίπαλος δεν είναι σε θέση να διακρίνει πότε το αποτέλεσμα προέρχεται από τη συνάρτηση μετάθεσης του κρυπτοσυστήματος και πότε όχι. Αντίθετα, για τιμές κοντά στη μονάδα, ο αντίπαλος εντοπίζει με επιτυχία αν το αποτέλεσμα προέρχεται από τη μετάθεση ή όχι. Όπως είναι φανερό από τον ορισμό, ο αντίπαλος μπορεί να έχει πλεονέκτημα κοντά στο **-1**. Πλεονέκτημα ίσο με **-1** σημαίνει ότι ο αντίπαλος κάνει πάντοτε λά-

θος. Αυτό όμως ισοδυναμεί με επιτυχία του αντιπάλου, αφού μπορεί κάλλιστα να ορισθεί ο αντίπαλος Α΄ ο οποίος δίνει την αντίθετη απάντηση από τον αντίπαλο Α.

Όπως αναφέραμε στο Κεφάλαιο 1, μια από τις βασικές αρχές της κρυπτογραφίας είναι η αρχή του Kerkhoff: ο αντίπαλος γνωρίζει τα πάντα γύρω από το κρυπτοσύστημά μας, εκτός από το κλειδί το οποίο χρησιμοποιούμε. Επομένως, μπορούμε να θεωρήσουμε ότι ο αντίπαλος μπορεί να κατασκευάσει ένα κρυπτοσύστημα όμοιο με αυτό που επιχειρεί να σπάσει. Ισοδύναμα, μπορούμε να υποθέσουμε ότι έχει στη διάθεσή του τη μετάθεση η οποία προσδιορίζεται από το κρυπτοσύστημα με το κλειδί, το οποίο δε γνωρίζει. Σε αυτό το σημείο εισάγεται και η έννοια του ***μαντείου*** (oracle). Ο όρος «μαντείο» δικαιολογείται αν αναλογισθούμε τη θέση του αντιπάλου ως προς τα χαρακτηριστικά του μαντείου. Ένα μαντείο είναι ένα σύστημα το οποίο περικλείει μυστικά μια συνάρτηση άγνωστη στον αντίπαλο. Η συνάρτηση μπορεί να είναι είτε από το σύνολο F^n, είτε από το σύνολο H^n, με μυστικό το κλειδί. Σε όλη τη διαδικασία, τα περιεχόμενα του μαντείου είναι σταθερά. Δηλαδή, για μια συγκεκριμένη «ερώτηση» (είσοδο), το μαντείο θα αποκρίνεται πάντοτε με την ίδια «απάντηση» (έξοδο). Κατά τη διάρκεια της διαδικασίας μπορούμε να διαθέτουμε στον αντίπαλο περισσότερα από ένα μαντεία. Έτσι ο αντίπαλος από τη θέση του μπορεί να θέτει ερωτήματα στο μαντείο και να δέχεται τις απαντήσεις, χωρίς όμως να γνωρίζει το περιεχόμενο του μαντείου και τον τρόπο με τον οποίο καταλήγει στην απάντηση.

Με την εισαγωγή του μαντείου στο μοντέλο μας, μπορούμε να παραμετροποιήσουμε το πλεονέκτημα του αντιπάλου, ως προς τον αριθμό των ερωτημάτων που έχει τη δυνατότητα να κάνει στο μαντείο. Έτσι όπως είναι φυσικό, για μεγάλο αριθμό ερωτημάτων, ο αντίπαλος θα μπορεί να διακρίνει αν το μαντείο κρύβει τη μετάθεση ή όχι. Επομένως, με παράμετρο τον αριθμό των ερωτημάτων, μπορούμε να προσδιορίσουμε το ανώτατο όριο του πλεονεκτήματος του αντιπάλου.

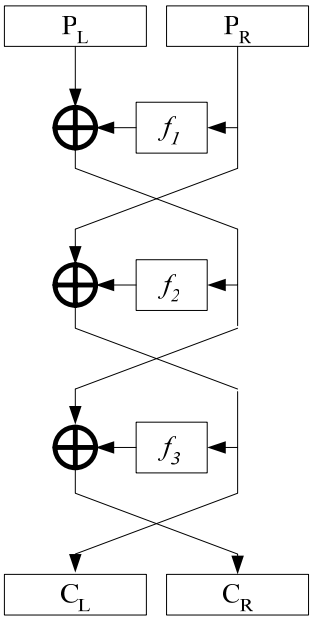
Λαμβάνοντας υπόψη τον αριθμό ερωτημάτων προς το μαντείο, το πλεονέκτημα του αντιπάλου ορίζεται ως:

$$\delta(q) = \max_{A}\{\delta(A)\}$$

το οποίο αντιστοιχεί στο μέγιστο πλεονέκτημα από τους αντιπάλους οι οποίοι θέτουν q ερωτήματα.

Ψευδοτυχαίες μεταθέσεις

Θεωρούμε το σύνολο των μεταθέσεων P^{2n} και επιλέγουμε το κρυπτοσύστημα που αποτελείται από δίκτυο Feistel τριών γύρων με συναρτήσεις γύρου $f_i: \{0,1\}\times\{0,1\}^n \rightarrow \{0,1\}^n$, για $1 \le i \le 3$ όπως φαίνεται στο Σχήμα 4.15. Σύμφωνα με την ιδιότητα του δικτύου Feistel, η κατασκευή μας είναι μετάθεση και ορίζεται από στοιχεία του P^{2n}. Πιο συγκεκριμένα, θεωρούμε ότι η κατασκευή Feistel αποτελεί μια ***ψευδοτυχαία μετάθεση***, όπου επιθυμούμε να υπολογίσουμε αν ο αντίπαλος μπορεί να τη διακρίνει από μια ***τυχαία συνάρτηση***. Η υπόθεση της τυχαίας συνάρτησης είναι ένα πολύ σημαντικό σημείο το οποίο θα ορισθεί παρακάτω.



Σχήμα 4.15 Δίκτυο Feistel τριών γύρων

Έστω ότι η συνάρτηση που υπολογίζει το δίκτυο Feistel τριών γύρων είναι η $h_{f_1,f_2,f_3}(\,)$, όπου οι συναρτήσεις γύρου είναι τυχαίες συναρτήσεις.

ΘΕΩΡΗΜΑ 4.1 Έστω A ένας αντίπαλος ο οποίος θέτει q ερωτήματα σε μαντείο. Τότε:

$$|\,\delta(A)\,| = |\,\Pr\{A(h_{f_1,f_2,f_3}) = 1 : f_1, f_2, f_3 \in F^n\} - \Pr\{A(f) = 1 : f \in F^{2n}\}\,| \le \frac{q^2}{2n}$$

Δηλαδή το πλεονέκτημα του αντιπάλου δεσμεύεται και είναι μικρότερο ή ίσο του λόγου του τετραγώνου των ερωτημάτων προς το μέγεθος του τμήματος του απλού κειμένου (ή του κρυπτοκειμένου). Η απόδειξη είναι καθαρά θεωρητική και παραλείπεται στο βιβλίο αυτό, αλλά ο αναγνώστης που ενδιαφέρεται μπορεί να ανατρέξει στη βιβλιογραφία (βλ. Luby & Rackoff, 1988). Το βασικό συμπέρασμα που προκύπτει είναι ότι για να είναι ένα δίκτυο Feistel αποδείξιμα ασφαλές, θα πρέπει να αποτελείται από τουλάχιστον τρεις γύρους, όπου η κάθε συνάρτηση γύρου είναι τυχαία και διαφορετική από τις υπόλοιπες.

Ψευδοτυχαίες συναρτήσεις

Η βασική υπόθεση είναι ότι οι συναρτήσεις γύρου είναι τυχαίες συναρτήσεις. Έστω η οικογένεια των συναρτήσεων f: $\{0, 1\}^k \times \{0, 1\}^n \to \{0, 1\}^n$, όπου η πρώτη είσοδος καθορίζει το κλειδί. Για ευκολία αναπαριστάνουμε την οικογένεια συναρ-

τήσεων με μέλη $f_k(x)$, όπου $x \in \{0, 1\}^n$. Η $f_k(x)$ είναι ψευδοτυχαία, αν ο αντίπαλος δεν είναι σε θέση να τη διακρίνει από μια τυχαία συνάρτηση f η οποία ανήκει στο σύνολο των συναρτήσεων (αντιστοιχίσεων) F^n.

Συνεπώς η ύπαρξη ψευδοτυχαίων μεταθέσεων συνδέεται με την ύπαρξη ψευδοτυχαίων συναρτήσεων. Οι ψευδοτυχαίες συναρτήσεις με τη σειρά τους συνδέονται με την ύπαρξη ψευδοτυχαίων γεννητριών που παρουσιάσαμε στην αρχή του κεφαλαίου.

Ψευδοτυχαίες γεννήτριες

Προτού προσδιορίσουμε την εξάρτηση των ψευδοτυχαίων συναρτήσεων με τις ψευδοτυχαίες γεννήτριες, θα ορίσουμε την ψευδοτυχαία γεννήτρια με βάση τον αντίπαλο και το πλεονέκτημά του.

Όπως παρουσιάσαμε στην αρχή του κεφαλαίου, μια τυχαία ακολουθία είναι αυτή η οποία περνάει όλους τους γνωστούς ελέγχους περί τυχαιότητας. Θεωρούμε λοιπόν ότι ο αντίπαλος έχει γνώση όλων των ελέγχων και μπορεί να τους εφαρμόζει στην ακολουθία. Ο αντίπαλος είναι ένας αλγόριθμος ο οποίος απαντάει με **1** αν ανακαλύψει (ή πιστεύει) ότι η ακολουθία που εξετάζει είναι ψευδοτυχαία, δηλαδή ότι δεν είναι τυχαία αλλά χρησιμοποιήθηκε κάποια συνάρτηση g για τη δημιουργία της, ή με **0** αν πιστεύει ότι η ακολουθία είναι τυχαία. Η συνάρτηση ψευδοτυχαίας ακολουθίας δέχεται μια μυστική είσοδο μεγέθους k bits και παράγει μια έξοδο μήκους L bits, όπου $k < L$.

ΟΡΙΣΜΟΣ 4.11 – Έστω η συνάρτηση $g: \{0, 1\}^k \to \{0, 1\}^L$ με $k < L$. Το πλεονέκτημα του αντιπάλου για να διακρίνει τα αποτελέσματα της g είναι:

$$\delta(A) = \Pr[A(y) = 1 : x \in \{0,1\}^k, y = g(x)] - \Pr[A(y) = 1 : y \in \{0,1\}^L].$$

Μπορούμε επίσης να θεωρήσουμε ότι η επιτυχία του αντιπάλου εξαρτάται από το χρόνο τον οποίο διαθέτει για να αναλύσει την ακολουθία. Θεωρητικά μετά από αρκετό χρόνο μπορούμε να υποθέσουμε ότι έχει ανακαλύψει τον έλεγχο με τον οποίο μπορεί να διακρίνει αν η ακολουθία είναι ψευδοτυχαία ή πραγματικά τυχαία:

$$\delta(t) = \max_A \{\delta(A)\},$$

όπου $\delta(t)$ το μέγιστο των πλεονεκτημάτων όλων των αντιπάλων που εκτελούνται σε χρόνο μικρότερο ή ίσο του t.

ΠΑΡΑΔΕΙΓΜΑ 4.10 – Κατασκευή ψευδοτυχαίας ακολουθίας από ψευδοτυχαία συνάρτηση. Το παράδειγμα αυτό παρατίθεται προκειμένου να δείξουμε τον τρόπο συλλογισμού που ακολουθείται για να συσχετίσουμε τις διαφορετικές κατασκευές (ακολουθίες, συναρτήσεις, μεταθέσεις). Ορισμένοι συσχετισμοί είναι πιο πολύπλοκοι από άλλους όσον αφορά την διαδικασία ανάλυσης απόδειξης, και γι αυτό

επιλέχθηκε μια σχετικά απλή περίπτωση, αυτή της δημιουργίας ψευδοτυχαίας ακολουθίας από ψευδοτυχαία συνάρτηση.

Έστω η ψευδοτυχαία συνάρτηση $f:\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$. Με βάση αυτήν τη συνάρτηση κατασκευάζουμε τη γεννήτρια ψευδοτυχαίας ακολουθίας $g:\{0,1\}^k \to \{0,1\}^L$, με:

$$g(k) = f_k(0) \,\|\, f_k(1) \,\|\, \ldots \,\|\, f_k(\lceil L/n \rceil - 1)\ [1..\mathrm{L}]$$

όπου || η συνένωση των δυαδικών λέξεων για τη δημιουργία λέξης πολλαπλάσιου μήκους, και [1..L] η επιλογή των L πρώτων δυαδικών ψηφιών, ώστε το αποτέλεσμα της συνάρτησης να είναι μήκους L.

Εφόσον η συνάρτηση f είναι ψευδοτυχαία, θα υπάρχει σχετικό μαντείο το οποίο διατίθεται στον αντίπαλο (της συνάρτησης). Έστω $A_f(\ )$ το μαντείο αυτό. Ο αντίπαλος A' της συνάρτησης, μπορεί να κατασκευασθεί από τον αντίπαλο A της γεννήτριας, ως εξής:

Αντίπαλος A':

1. Έστω $N = \lceil L/n \rceil$
2. Έστω $y = A_f(0) \| A_f(1) \| \ldots A_f(N)[1..L]$
3. Εκτέλεσε τον $A(y)$
4. Επέστρεψε το αποτέλεσμα του αντιπάλου A ως αποτέλεσμα του A'

Από την περιγραφή του αντιπάλου της συνάρτησης, προκύπτει ότι απαιτούνται $q = \lceil L/n \rceil$ ερωτήματα στο μαντείο, ενώ ο χρόνος που απαιτείται είναι ο χρόνος του αντιπάλου A της γεννήτριας συν το χρόνο για την απάντηση των ερωτημάτων, ο οποίος είναι ανάλογος του L, επομένως:

$$t_{A'} = t_A + cL$$

για κάποιο σταθερό c. Μας μένει να υπολογίσουμε και το πλεονέκτημα του A'. Σύμφωνα με τον Ορισμό 4.11, το πλεονέκτημα του αντιπάλου της γεννήτριας είναι:

$$\delta(A) = \Pr[A(y) = 1 : x \in \{0,1\}^k, y = g(x)] - \Pr[A(y) = 1 : y \in \{0,1\}^L].$$

Παρόμοια ορίζουμε το πλεονέκτημα του αντιπάλου A':

$$\delta(A') = \Pr[A'(f_y) = 1 : y \in \{0,1\}^k] - \Pr[A'(y) = 1 : y \in \{0,1\}^n]$$

Όσον αφορά τον A', το μαντείο που του παρέχεται περιέχει είτε μια πραγματικά τυχαία συνάρτηση, ή μια ψευδοτυχαία συνάρτηση, δηλαδή $A_f = f$ ή $A_f = f_k$. Στην πρώτη περίπτωση θα είναι:

$$\Pr[A'(y) = 1 : y \in \{0,1\}^n] = \Pr[A(y) = 1 : y \in \{0,1\}^L],$$

δηλαδή η πιθανότητα να απαντήσει ο αντίπαλος *A΄* ότι η συνάρτηση είναι τυχαία είναι ίδια με την πιθανότητα να απαντήσει ο αντίπαλος *A* ότι η γεννήτρια είναι τυχαία (αφού οι απαντήσεις των *A΄* και *A* ταυτίζονται).
Παρόμοια, αν το μαντείο περιέχει τη συνάρτηση $A_f = f_k$, τότε:

$$\Pr[A'(f_y) = 1 : y \in \{0,1\}^k] = \Pr[A(y) = 1 : x \in \{0,1\}^k, y = g(x)],$$

δηλαδή η πιθανότητα να εντοπίσει ο αντίπαλος *A΄* ότι η συνάρτηση είναι ψευδοτυχαία είναι ίδια με την πιθανότητα να εντοπίσει ο *A* ότι η γεννήτρια είναι ψευδοτυχαία.
Από τα παραπάνω προκύπτει ότι $\delta(A') = \delta(A)$. Δηλαδή, ο αντίπαλος της ψευδοτυχαίας συνάρτησης βρίσκεται ακριβώς στην ίδια κατάσταση με τον αντίπαλο της ψευδοτυχαίας γεννήτριας, από πλευράς πλεονεκτήματος.

Όροι-κλειδιά του κεφαλαίου

- ψευδοτυχαίες ακολουθίες
- καταχωρητές ολίσθησης με ανάδραση
- γραμμική πολυπλοκότητα
- μονόδρομες συναρτήσεις
- μονόδρομες hash και ανθεκτικότητα σε συγκρούσεις
- δίκτυα αντικατάστασης-μετάθεσης
- κουτιά αντικατάστασης
- δίκτυα Feistel

4.6. Ασκήσεις

1. Με τον έλεγχο της συχνότητας, εξετάστε αν οι πηγή που παρήγαγε την παρακάτω δυαδική ακολουθία είναι πολωμένη:
   [10101001011101010001000001]
2. Εξετάστε με τον έλεγχο της αυτοσυσχέτισης την κατανομή των άσσων και μηδενικών, στις παρακάτω ακολουθίες:
   [1110001111000111000], [11010010001101101],
   [0111101011000010111], [10110111011110011].
3. Εξετάστε με βάση τα κριτήρια του Golomb, αν οι παρακάτω δυαδικές ακολουθίες είναι ψευδοτυχαίες:
   [100110011111101], [000100110101111],
   [011011000101010], [110001010001011].
4. Υπολογίστε τους 20 πρώτους όρους των ακολουθιών που παράγουν οι γραμμικοί καταχωρητές με χαρακτηριστικά πολυώνυμα:
   $f = 1 + x^2 + x^3 + x^7$ $f = 1 + x^2 + x^3 + x^5 + x^{16}$,

με αρχική κατάσταση το διάνυσμα (**0**, **1**, **1**, …, **1**). Θεωρήστε ότι το μέγεθος του καταχωρητή είναι ίσο με το βαθμό του πολυωνύμου.

5. Κρυπταναλύστε τις παρακάτω ακολουθίες, προσδιορίζοντας γραμμικούς καταχωρητές ανάδρασης οι οποίοι να μπορούν να παράγουν τις ακολουθίες αυτές. Στη συνέχεια χρησιμοποιείστε τους γραμμικούς καταχωρητές που προσδιορίσατε για να προβλέψετε το επόμενο bit της ακολουθίας.
   [1010110010], [10011101001101],
   [0001010111], [100000001].
6. Έστω η κρυπτογραφική μονόδρομη hash h: $\{0, 1\}^* \rightarrow \{0, 1\}^{32}$. Εκτιμήστε τον αριθμό των μηνυμάτων που απαιτούνται προκειμένου η πιθανότητα, οποιωνδήποτε δύο από τα μηνύματα αυτά να έχουν την ίδια σύνοψη, να είναι 0,75.
7. Έστω το κουτί αντικατάστασης

Είσοδος i	$S(i)$	Είσοδος i	$S(i)$
000	101	100	111
001	100	101	000
010	011	110	100
011	010	111	010

   (α) Δείξτε ότι το κουτί S δεν είναι αντιστρέψιμο.
   (β) Δείξτε ότι δεν ισχύει η ιδιότητα $S(x_1 \oplus x_2) = S(x_1) \oplus S(x_2)$.
   (γ) Υπολογίστε τη διάχυση των bits εισόδου, για το κάθε bit χωριστά (σημ. η μέγιστη διάχυση ενός bit εισόδου είναι ίση με 3, εφόσον έχει τη δυνατότητα να επηρεάσει και τα 3 bits εξόδου).
8. Έστω ένα δίκτυο Feistel σημαίνοντος στόχου, με συνάρτηση γύρου:
   $f : \{0,1\}^{16} \rightarrow \{0,1\}^{48}$
   (α) Αν το δίκτυο είναι τέλειο, ποιο είναι το μέγεθος της εισόδου και της εξόδου;
   (β) Αν υποθέσουμε ότι η συνάρτηση γύρου f είναι ασφαλής, ποιος είναι ο ελάχιστος αριθμός γύρων, προκειμένου το δίκτυο Feistel να αποτελεί ασφαλές κρυπτοσύστημα;
   (γ) Αν το δίκτυο είναι ατελές με μηδενικό τμήμα ίσο με 16 bit, ποιο είναι το μέγεθος της εισόδου και της εξόδου;
   (δ) Στο δίκτυο της περίπτωσης (γ), ποιος είναι ο ελάχιστος αριθμός γύρων για ένα ασφαλές κρυπτοσύστημα βασιζόμενο στο δίκτυο Feistel;