Κεφάλαιο 16

Κρυπτογραφία και Ασφάλεια

16.1 Ιστορική αναδρομή

Η τέχνη της κρυπτογραφίας ξεκίνησε εδώ και 2500 χρόνια, το λιγότερο και έπαιξε σημαντικό ρόλο στην ιστορία απο τότε. Στην αρχαία Ελλάδα, οι έφοροι της Σπάρτης επικοινωνούσαν με τους στρατηγούς χρησιμοποιώντας μακριές και στενές κορδέλες τις οποίες τύλιγαν γύρω από μια σκυτάλη (κύλινδρο) και μετά γράφαν το μήνυμα κατά μήκος της σκυτάλης. Για να διαβάσει κάποιος το μήνυμα, έπρεπε να έχει μια παρόμοια σκυτάλη με αυτή που είχε χρησιμοποιηθεί για την κωδικοποίηση και να τυλίξει την κορδέλα γύρω από τη σκυτάλη με τον ίδιο τρόπο. Αυτό το σύστημα (διπλής κατεύθυνσης) κρυπτογραφίας είναι ένα κλασικό σύστημα με ένα κλειδί (τη σκυτάλη).

Ο Ιούλιος Καίσαρας επικοινωνούσε με τους φίλους του αντικαθιστώντας κάθε γράμμα με ένα άλλο, το οποίο προέκυπτε με ολίσθηση κατά k βήματα στο αλφάβητο. Αυτό είναι ένα από τα πιο απλά, εύκολα αλλά και ανασφαλή κρυπτοσυστήματα που έχουν προταθεί.

Οι Βενετοί ήταν οι πρώτοι που χρησιμοποίησαν κρυπτογραφία συστηματικά, από το 13ο αιώνα, για διπλωματική αλληλογραφία. Οι πρώτες δημοσιεύσεις (στα λατινικά) περί κρυπτογραφίας φάνηκαν το 1500 ("Στεγανογραφία") και το 1518 από τον αββά Ιωάννη Τριθέμιο και αργότερα δημοσιεύτηκε το "Περι κρυπτικών συμβόλων και γραμμάτων" από τον J. B. Porta (1538 - 1615, Ιταλό φυσικό και μαθηματικό). Από τότε η κρυπτογραφία έγινε αντικείμενο ιδιαίτερου ενδιαφέροντος και απέκτησε εφαρμογές. Οι αλχημιστές χρησιμοποιούσαν σύμβολα για να κρυπτογραφήσουν τους τύπους τους, αλλά και πολλοί φιλόσοφοι ενδιαφέρθηκαν για την κρυπτογραφία: Ο Sir Francis Bacon (1561 - 1626) επινόησε ένα σύστημα κρυπτογράφησης όπου κάθε γράμμα αντικαθίσταται με μια λέξη πέντε γραμμάτων και ο Leonardo Da Vinci (1452 - 1519) χρησιμοποιούσε μια μέθοδο κρυπτογράφησης με καθρέπτη.

Ο Edgar Allan Poe (1809-1849) στο κλασικό διήγημα "Το χρυσό έντομο" ("The Gold Bug") που δημοσίευσε το 1843, εξηγεί τις βασικές αρχές σπασίματος των κωδίκων και υποστηρίζει την άποψη ότι ο ανθρώπινος νους μπορεί να σπάσει οποιοδήποτε κρυπτογραφημένο κείμενο που η ανθρώπινη ευρηματικότητα μπορεί να επινοήσει. Ακόμη περιγράφει ένα σύστημα με το οποίο κάθε κρυπτογραφημένο κείμενο που προέρχεται από μια ευρωπαϊκή γλώσσα μπορεί να

αποκρυπτογραφηθεί, αν έχει κρυπτογραφηθεί με αλφαβητική αντικατάσταση, μετρώντας τη συχνότητα των γραμμάτων της γλώσσας.

Ίσως από τα διασημότερα κρυπτογραφήματα, το *σημείωμα του Zimmerman* (*the Zimmerman Note*) ώθησε τις ΗΠΑ στον πρώτο παγκόσμιο πόλεμο. Όταν το κρυπτογράφημα αποκρυπτογραφήθηκε το 1917, οι Αμερικανοί έμαθαν ότι η Γερμανία είχε προσπαθήσει να πείσει το Μεξικό να μπει στον πόλεμο με το μέρος της, υποσχόμενη παραχωρήσεις εδαφών των ΗΠΑ στο Μεξικό.

Τον ίδιο περίπου καιρό, ο Gilbert S. Vernam της AT&T ανέπτυξε τον πρώτο πραγματικά αθραυστο κώδικα που ονομάστηκε βέβαια *κρυπτογράφηση Vernam* (*The Vernam Cipher*). Μια ξεχωριστή ιδιότητα αυτού του κώδικα είναι η απαίτηση για ένα κλειδί με μήκος όσο και το μήνυμα που πρέπει να μεταδοθεί και το οποίο δεν ξαναχρησιμοποιείται για την αποστολή άλλου μηνύματος (η κρυπτογράφηση Vernam είναι γνωστή επίσης και ως *κρυπτογράφηση με μπλοκάκι μιας χρήσης* (*one-time-pad*) από την πρακτική της προμήθευσης κατασκόπων με το κείμενο-κλειδί γραμμένο σ'ένα μπλοκάκι του οποίου κάθε κομμάτι χρησιμοποιείται μια φορά και μετά καταστρέφεται). Η ανακάλυψη του συστήματος αυτού δεν εκτιμήθηκε ιδιαίτερα εκείνη την εποχή, πιο πολύ επειδή δεν είχε αποδειχτεί ακόμη ότι είναι άθραυστος κώδικας και επειδή η απαίτηση για πολλά και μεγάλα κλειδιά την έκαναν μη πρακτική για γενική χρήση. Εξαιτίας των μη πρακτικών απαιτήσεων της κρυπρογράφησης Vernam, άλλες (πιο αδύνατες) μέθοδοι συνεχισαν να χρησιμοποιούνται ευρέως. [1] Έτσι, κατά το δεύτερο παγκόσμιο πόλεμο, οι Σύμμαχοι ήταν σε θέση να αποκρυπτογραφούν τα περισσότερα από τα μυστικά μηνύματα που στέλνονταν από τους Γερμανούς. Η εγγενής δυσκολία του σπασίματος των ολοένα και πιο περίπλοκων κρυπτογραφικών μεθόδων ήταν μάλιστα ένας από τους παράγοντες που προώθησε την ανάπτυξη των ηλεκτρονικών υπολογιστών.

Η περίφημη *Μηχανή-Αίνιγμα* (*Enigma*) που χρησιμοποιήθηκε απο τους Γερμανούς κατα το δεύτερο παγκόσμιο πόλεμο για κρυπτογράφηση ραδιοτηλεπικοινωνιών πυροδότησε μια από τις πιο έντονες προσπάθειες αποκρυπτογράφησης στην ιστορία. Ο κώδικας Αίνιγμα θυμίζει έναν παλιότερο κώδικα τύπου Vigenére αλλά είναι πολύ πιο πολύπλοκος. Μια βασική ιδιότητα της μηχανής αυτής ήταν η αυτο-αντιστροφή: εάν το κωδικοποιημένο κείμενο δινόταν ώς είσοδος στη μηχανή, τότε η έξοδος θα ήταν το αρχικό μήνυμα (αν φυσικά η μηχανή είχε την ίδια αρχική κατάσταση με τη μηχανή που είχε κάνει την κωδικοποίηση). Παρόλο που αυτό αποτελούσε τρομερή ευκολία για τους χειριστές της μηχανής, αποδείχτηκε ότι ήταν και μεγάλη αδυναμία του κώδικα Αίνιγμα. Πριν τον πόλεμο, η γαλλική αντικατασκοπεία είχε αποκτήσει αντίγραφα των εντολών της μηχανής-Αίνιγμα και πέρασε την πληροφορία αυτή στους Πολωνούς που υπέκλεπταν και ανέλυαν τις γερμανικές ραδιο-επικοινωνίες. Με τη βοήθεια των εντολών αυτών, οι Πολωνοί κρυπταναλυτές μπόρεσαν να συμπεράνουν τη συνδεσμολογία-καλωδίωση της μηχανής, οπότε έγινε δυνατό να διαβάζονται τα κρυπτογραφημένα κείμενα, αρκεί να είναι γνωστή η αρχική κατάσταση της μηχανής. Παρόλο που οι Βρετανοί τα έμαθαν όλα αυτά απο τους Πολωνούς, είχαν μικρή αξία γι'αυτούς επειδή οι Γερμανοί έκαναν κάποιες τροποποιήσεις στη μηχανή πριν τον πόλεμο. Οι Βρετανοί συγκέντρωσαν μια ομάδα κρυπταναλυτών και μαθηματικών, συμπεριλαμβανομένου και του Alan Turing, σε μια βικτωριανή έπαυλη στο Buckinghamshire που

[1] Αξίζει πάντως να αναφερθεί ότι όταν το 1967 ο στρατός της Βολιβίας συνέλαβε και εκτέλεσε τον επαναστάτη Che Guevara, βρήκαν στην κατοχή του ένα χαρτί που έδειχνε πως προετοίμαζε ένα μήνυμα για αποστολή στον Κουβανό πρόεδρο Fidel Castro. Ο Che Guevara χρησιμοποιούσε τον άσπαστο κώδικα Vernam που είχε εφεύρει ο Vernam 1918.

ονομαζόταν Bletcley Park. Χρησιμοποιώντας τις πληροφορίες των Πολωνών, η ομάδα βάσισε τις προσπάθειές της στη λεγόμενη μέθοδο πιθανής λέξης. Η μέθοδος αυτή βασίζεται στο γεγονός ότι σε κάποιες περιπτώσεις μια συγκεκριμένη ακολουθία συμβόλων σχεδόν σίγουρα αντιπροσωπεύει μια γνωστή λέξη. Μαντεύοντας σωστά μερικές από τις κρυπτογραφημένες λέξεις του κρυπτοκειμένου, μπορούσαν να καθορίζουν τη συνδεσμολογία της μηχανής, δοκιμάζοντας όλες τις πιθανές συνδεσμολογίες και προσδιορίζοντας ποια είχε ως αποτέλεσμα τα υποτιθέμενα ζευγάρια κρυπτογραφημένων-αποκρυπτογραφημένων λέξεων. Ο Turing αντιλήφθηκε ότι μόνο μια αυτόματη και σχετικά γρήγορη μηχανή θα μπορούσε να τα βγάλει πέρα με τις δοκιμές, όποτε και οδηγήθηκε στην κατασκευή ενός εξομοιωτή της μηχανής-Αίνιγμα με το όνομα Bombe.

Η σημερινή μορφή των κρυπτογραφικών συστημάτων έχει καθοριστεί σε πολύ μεγάλο βαθμό από δύο, κεφαλαιώδους σημασίας για την κρυπτογραφία και τις επικοινωνίες γενικότερα, επιστημονικές εργασίες Kerchoff, Shannon, που δημοσιεύτηκαν στα 1883 και 1949 αντίστοιχα. Στην πρώτη, ο Kerchoffs έθεσε τη βασική σχεδιαστική αρχή που έκτοτε διέπει κάθε κρυπτογραφικό σύστημα, σύμφωνα με την οποία η ασφάλεια ενός συστήματος πρέπει να έγκειται *μόνο* στη μυστικότητα του κλειδιού και να μην εξαρτάται από τη μυστικότητα του αλγορίθμου κρυπτογράφησης. Η δεύτερη εργασία ανήκει στο θεμελιωτή της Θεωρίας Πληροφορίας Claude Shannon. Στην εργασία αυτή η κρυπτογραφία μετατρέπεται σε αυστηρό επιστημονικό πεδίο, όπου ορίζεται η έννοια του κρυπτοσυστήματος και η απόλυτη ασφάλεια. Η εργασία αυτή του Shannon αποτέλεσε ισχυρή κινητήρια δύναμη για την ταχεία εξέλιξη της έρευνας στο χώρο της κρυπτογραφίας, η οποία έλαβε χώρα στο δεύτερο μισό του εικοστού αιώνα και συνεχίζεται μέχρι σήμερα. Όλοι οι σύγχρονοι κρυπτογραφικοί αλγόριθμοι σχεδιάζονται υπό το πρίσμα των εννοιών που εισήγαγε ο Shannon. Σημαντική τομή επίσης στο χώρο της κρυπτογραφίας αποτέλεσε η εργασία των Diffie-Hellman το 1976 Diffie, όπου προτάθηκε μία διαφορετική τεχνική κρυπτογράφησης που καλείται *κρυπτογραφία δημοσίου κλειδιού*, η οποία επιλύει προβλήματα που σχετίζονται τόσο με την ασφαλή ανταλλαγή του κλειδιού όσο και με την πιστοποίηση της ταυτότητας των χρηστών

Το ακαδημαϊκό ενδιαφέρον στην κρυπτολογία αναπτύχθηκε πιο έντονα το 1976, όταν οι Whitfield Diffie, Martin E. Hellman και Ralph C. Merkle (τότε στο Stanford University) ανακάλυψαν τις αρχές της κρυπτογραφίας δημόσιου κλειδιού (public key cryptography) [2]. Το 1977 οι Ronald L. Rivest, Adi Shamir και Leonard M. Adleman (τότε στο MIT) σχεδίασαν μια πρακτική υλοποίηση της κρυπτογραφίας δημοσίου κλειδιού, τον αλγόριθμο RSA (βλέπε [10]). Το 1982 ο Shamir έσπασε ένα από τα πρώτα συστήματα κρυπτογράφησης δημοσίου κλειδιού, το κρυπτοσύστημα σακιδίου (knapsack cipher).

Στις αρχές της δεκαετίας του 1980, οι φυσικοί ανέπτυξαν κρυπτογραφικά σχήματα βασισμένα στην κβαντομηχανική.

Θεωρούμε ότι αξίζει εδώ μια ειδική αναφορά μιας άλλης επιστημονικής περιοχής, η οποία συγγενεύει αρκετά με την κρυπτογραφία: της προσπάθειας αποκρυπτογράφησης των αρχαίων γραφών. Είναι χαρακτηριστικό ότι οι πλέον ρηξικέλευθες ανακαλύψεις σε αυτόν τον τομέα δεν έχουν γίνει από θεωρητικούς επιστήμονες αρχαιολόγους, φιλόλογους, αιγυπτιολόγους, κλασικιστές, κλπ, αλλά από μηχανικούς και θετικούς επιστήμονες οι οποίοι έδειξαν ερασιτεχνικό ενδιαφέρον για τα προβλήματα της αποκρυπτογράφησης και τα αντιμετώπισαν με μαθηματικό τρόπο σκέψης.

Η πλέον εντυπωσιακή σχετική ανακάλυψη είναι η αποκρυπτογράφηση της Γραμμικής γραφής Β′ των πινακίδων του μυκηναϊκού πολιτισμού από τον Γάλλο αρχιτέκτονα Michel Ventris κατά

τη δεκαετία του 1950. Μέχρι τότε οι αρχαιολόγοι, σε μια αξιοπερίεργη επίδειξη επιστημονικής πλάνης, θεωρούσαν ότι η γραφή αυτή ανήκε σε σημιτική γλώσσα, όχι ελληνική, παρόλο που ήταν προφανές ότι τα μυκηναϊκά αρχαιολογικά ευρήματα ανήκαν στον πρώιμο πολιτισμό των Ελλήνων και σχετιζόταν με το ιστορικό γεγονός του Τρωικού Πολέμου και πλήθος ελληνικών μυθολογικών παραδόσεων. Ο Ventris όμως βασίστηκε στην εκ των προτέρων παραδοχή ότι η γλώσσα των μυκηναϊκών πινακίδων είναι ελληνική και κατέληξε έτσι στην πλήρη και αναμφισβήτητη αποκρυπτογράφησή της. Αυτή η ανακάλυψη επιβεβαίωσε την ελληνικότητα του μυκηναϊκού πολιτισμού και διέψευσε τις απόψεις περί ελεύσεως των Ελλήνων στην Ελλάδα μετά το 12ο αιώνα π.Χ., οι οποίες επικρατούσαν τότε.

Η Γραμμική γραφή Α′ του μινωικού πολιτισμού, που δεν έχει πλήρως αποκρυπτογραφηθεί, είναι μάλλον επίσης ελληνική και συγγενεύει με τη Γραμμική Β′, καθώς και με συστήματα γραφής των Χετταίων της Ανατολικής Μικράς Ασίας, των Ετρούσκων της Βόρειας Ιταλίας, των Λυδών, των Λυκών και των Κάρων της Δυτικής Μικράς Ασίας.

16.2 Κρυπτογραφία - Μια εισαγωγή

Με τον όρο κρυπτολογία αναφερόμαστε τόσο στην κρυπτογραφία όσο και στην κρυπτανάλυση: Η κρυπτογραφία ασχολείται με το σχεδιασμό κρυπτοσυστημάτων, ενώ η κρυπτανάλυση μελετά το σπάσιμο των κρυπτοσυστημάτων.

Ένα κρυπτοσύστημα, γενικά, αποτελείται από δύο αλγορίθμους: έναν αλγόριθμο κρυπτογράφησης ή κωδικοποίησης (encryption or enciphering algorithm) E και έναν αλγόριθμο αποκρυπτογράφησης ή αποκωδικοποίησης (decryption or deciphering algorithm) D. (Τυπικός ορισμός του όρου κρυπτοσύστημα δίνεται στο κεφάλαιο 4) Το αρχικό κείμενο (plaintext - απλό κείμενο) είναι το κείμενο (μήνυμα…) προς κρυπτογράφηση. Χρησιμοποιώντας το αρχικό κείμενο για είσοδο του αλγορίθμου κρυπτογράφησης, παίρνουμε στην έξοδο το κρυπτοκείμενο (cryptotext ή ciphertext). Ο αλγόριθμος αποκρυπτογράφησης (η αντίστροφη διαδικασία δηλαδή) χρησιμοποιεί για είσοδο το κρυπτοκείμενο και εξάγει το αντίστοιχο αρχικό κείμενο.

Τα κρυπτοσυστήματα μπορούν να ταξινομηθούν ανάλογα με τον αριθμό των κλειδιών που χρησιμοποιούν:

- Κανένα κλειδί: Αν δεν χρησιμοποιούνται καθόλου κλειδιά, τότε το όλο κρυπτοσύστημα βασίζεται στον αλγόριθμο κρυπτογράφησης και αποκρυπτογράφησης. Αυτός ο αλγόριθμος θα πρέπει να κρατείται μυστικός, δηλαδή να είναι γνωστός μόνο σε εκείνους που είναι υπεύθυνοι για τα κρυπτογραφημένα κείμενα.

- Ένα κλειδί: Κλασική (διπλής κατεύθυνσης) κρυπτογραφία: Οι αλγόριθμοι E και D χρειάζονται μια παράμετρο k, η οποία ονομάζεται κλειδί (κρυπτογράφησης-αποκρυπτογράφησης). Θα συμβολίζουμε τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης με E_k και D_k αντίστοιχα. Ο αλγόριθμος κρυπτογράφησης-αποκρυπτογράφησης μπορεί να κοινοποιηθεί (να γίνει γνωστός σε όλους) αλλά το κλειδί κρυπτογράφησης θα πρέπει να είναι μυστικό.

- Δύο κλειδιά: Η κρυπτογραφία με δημόσιο κλειδί (ή μονής κατεύθυνσης κρυπτογραφία):

Οι αλγόριθμοι για κρυπτογράφηση και αποκρυπτογράφηση χρησιμοποιούν διαφορετικές παραμέτρους (κλειδιά): Ο αλγόριθμος κρυπτογράφησης χρησιμοποιεί το κλειδί κρυπτογράφησης k (το οποίο μπορεί να κοινοποιηθεί - δημόσιο κλειδί), και ο αλγόριθμος αποκρυπτογράφησης χρησιμοποιεί το κλειδί αποκρυπτογράφησης k', που θα πρέπει να είναι μυστικό.

Ο Sir Francis Bacon (1561-1626) πρότεινε τρεις γενικές απαιτήσεις τις οποίες ένα κρυπτοσύστημα θα πρέπει να πληροί:

1. Δεδομένων των αλγορίθμων κρυπτογράφησης και του αρχικού κείμενου θα πρέπει να είναι εύκολος ο υπολογισμός του κρυπτοκειμένου. (Δεδομένων των E_k και x να είναι εύκολο να υπολογιστεί το $E_k(x)$).

2. Αν είναι γνωστό μόνο το κρυπτοκείμενο, χωρίς να είναι γνωστό το D_k (δηλαδή ο αλγόριθμος ή το κλειδί αποκρυπτογράφησης), θα πρέπει να είναι αδύνατο να βρεθεί το αρχικό κείμενο.

3. Το κρυπτοκείμενο δεν θα πρέπει να είναι ύποπτο: να δείχνει αθώο.

Η απαίτηση 3 (μπορεί να επιτευχθεί χρησιμοποιώντας τη μέθοδο παρεμβολής σκουπιδιών - βλέπε παράδειγμα 1.2) δεν θεωρείται σημαντική πλέον, καθώς τόσο τα αρχικά κείμενα όσο και τα κρυπτοκείμενα αναπαρίστανται ως δυαδικές ακολουθίες οι οποίες από μόνες τους δείχνουν αρκετά αθώες. Οι απαιτήσεις (1) και (2) μπορούν να διατυπωθούν χρησιμοποιώντας ορολογία από την θεωρία πολυπλοκότητας: Η κρυπτογράφηση να είναι εύκολη (με χαμηλό πολυωνυμικό χρόνο, γραμμικό χρόνο), ενώ η κρυπτανάλυση να είναι υπολογιστικά απρόσιτη.

Η σύγχρονη κρυπτογραφία θεμελιώνεται πάνω στη θεωρία της υπολογιστικής πολυπλοκότητας. Ένα σύστημα θεωρείται *ασφαλές* όταν έχει αποδειχτεί κάτω όριο για την κρυπτανάλυσή του. Σημειώνουμε ότι κατά το σχεδιασμό ενός κρυπτοσυστήματος, μας ενδιαφέρουν τα κάτω όρια (Ω) ή η μέση πολυπλοκότητα του αντιστοίχου προβλήματος κρυπτανάλυσης, και όχι η πολυπλοκότητα της χειρότερης περίπτωσης (άνω όρια - O).

Η κρυπτανάλυση είναι δυνατόν να είναι είτε παθητική (υποκλοπή: ο κρυπταναλυτής προσπαθεί να αποκρυπτογραφήσει μηνύματα, να βρει κλειδιά, …) ή ενεργητική (παρεμβολή: ο κρυπταναλυτής παραποιεί δεδομένα που διαβιβάζονται, γράφει και διαβιβάζει δικά του κείμενα, ξαναδιαβιβάζει παλιό κρυπτοκείμενο, …)

Η κρυπτανάλυση ενός συστήματος (με κλειδί) μπορεί να ξεκινήσει από διαφορετικά αρχικά σενάρια:

- Το κρυπτοκείμενο μόνο: Μόνο το κρυπτοκείμενο είναι γνωστό στον κρυπταναλυτή.
- Γνωστό αρχικό κείμενο: Ο κρυπταναλυτής γνωρίζει κάποια ζευγάρια $(x, E_k(x))$ (αρχικών κειμένων και των αντιστοίχων κρυπτοκειμένων) και προσπαθεί να βρει το κλειδί k.
- Επιλεγμένο αρχικό κείμενο: Μερικά ζευγάρια $(x, E_k(x))$ είναι γνωστά στον κρυπταναλυτή όπου, επιπλέον, το αρχικό κείμενο x έχει επιλεγεί από τον ίδιο τον κρυπταναλυτή.

- Επιλεγμένο κρυπτοκείμενο: Μερικά ζευγάρια $(x, y = E_k(x))$ είναι γνωστά στον κρυπταναλυτή όπου, επιπλέον, το κρυπτοκείμενο y έχει επιλεγεί από τον ίδιο τον κρυπταναλυτή.
- Κλειδί κρυπτογράφησης: Ο κρυπταναλυτής γνωρίζει το κλειδί k, και συνεπώς και τη μέθοδο κρυπτογράφησης E_k, και προσπαθεί να βρει το κλειδί k' και άρα τη μέθοδο αποκρυπτογράφησης $D_{k'}$. (Αυτό το σενάριο είναι τυπικό για τα κρυπτοσυστήματα δημοσίου κλειδιού).

Οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης είναι γνωστοί στον κρυπταναλυτή και στα τέσσερα παραπάνω σενάρια — όχι όμως και το κλειδί αποκρυπτογράφησης.

Οι κρυπταναλυτικές επιθέσεις εναντίον κλασικών συστημάτων βασίζονται γενικά στη θεωρία πιθανοτήτων, στη στατιστική, στη γραμμική άλγεβρα, στην αφηρημένη άλγεβρα (θεωρία ομάδων) και στη θεωρία πολυπλοκότητας, ενώ η κρυπτανάλυση των συστημάτων δημοσίου κλειδιού βασίζεται κυρίως στη θεωρία αριθμών και στη θεωρία υπολογιστικής πολυπλοκότητας.

Ένας σημαντικός παράγοντας για την κρυπτανάλυση είναι η επιπλέον πληροφορία που διαθέτει ο κρυπταναλυτής (side information): Ο κρυπταναλυτής μπορεί να είναι οικείος με συγκεκριμένα στιγμιότυπα του συστήματος που σκοπεύει να σπάσει, ή ίσως να μπορεί να κάνει μερικές παραδοχές για το κρυπτοκείμενο, που θα του δώσουν ένα μεγάλο πλεονέκτημα στην επίθεσή του εναντίον του συστήματος. Για παράδειγμα η επίθεση εναντίον του γερμανικού συστήματος "Αίνιγμα" (Enigma), βασίστηκε στη θεώρηση ότι κάποια λέξη στο κρυπτοκείμενο θα έπρεπε να αντιστοιχεί στη λέξη "Unterseeboot" (υποβρύχιο). Ένα άλλο παράδειγμα επιπλέον πληροφόρησης είναι το ακόλουθο:

Θεωρήστε τον ακόλουθο γρίφο. Ξεδιαλύνετε κάθε έναν από τους εξής αναγραμματισμούς:

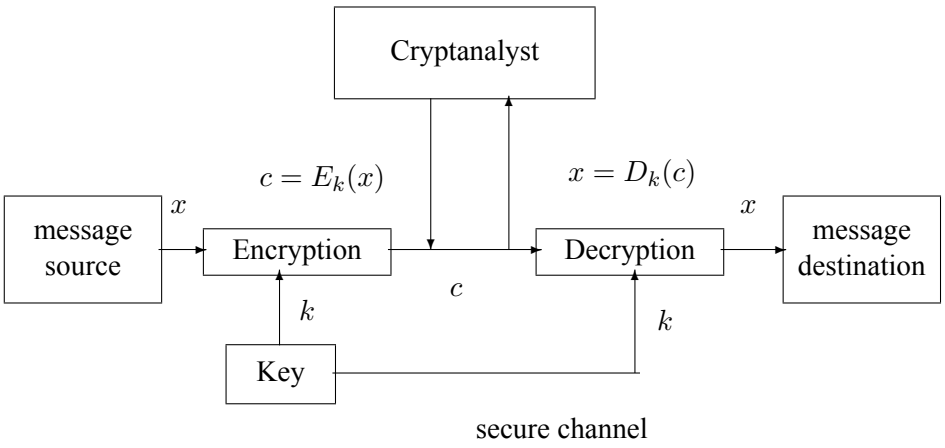
```
  DFOR    STOUL  IIBAGONMRLH  ECSEEMDR
IAERFRR  GEDOD    LADCLIAC    RITSAAEM
```

Δεν είναι δύσκολο να αναγνωρίσετε τις λέξεις, αλλά ο γρίφος γίνεται αρκετά εύκολος αν χρησιμοποιήσουμε την επιπλέον πληροφορία-υπόδειξη: "οι λέξεις αντιστοιχούν σε ονόματα αυτοκινήτων"

16.3 Κλασικά Συστήματα

Στην κλασική διπλής κατεύθυνσης κρυπτογραφία, οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης είναι γνωστοί σε όλους, και το ίδιο κλειδί χρησιμοποιείται και για τις δύο κατευθύνσεις (κρυπτογράφηση-αποκρυπτογράφηση). Με άλλα λόγια, στα κλασικά συστήματα, η αποκρυπτογράφηση είναι εύκολη αν το κλειδί κρυπτογράφησης είναι γνωστό. Αντίθετα, στην κρυπτογραφία δημοσίου κλειδιού το κλειδί k μπορεί με ασφάλεια να δημοσιοποιηθεί χωρίς να αποκαλυφθεί το κλειδί k'. Για αυτό το λόγο τα κλασικά συστήματα αναφέρονται επίσης και ως *συμμετρικά* ή *διπλής κατεύθυνσης συστήματα*, και τα συστήματα δημοσίου κλειδιού ως *μη-συμμετρικά* ή *μονής κατεύθυνσης* συστήματα (αυτό σημαίνει ότι η διαδικασία κρυπτογράφησης είναι μονής κατεύθυνσης - δεν μπορεί εύκολα να αντιστραφεί).

Μια (πολύ παλιά) κατηγοριοποίηση των κλασικών κρυπτοσυστημάτων είναι σε συστήματα *αντικατάστασης (substitution)* και *μετάθεσης (permutation)* (ή *αναδιάταξης (transposition)*).



Σχήμα 16.1: Συμβατικά (κλασικά) κρυπτοσυστήματα διπλής κατεύθυνσης

Στα συστήματα αντικατάστασης (substitution ciphers), τα γράμματα του αρχικού κειμένου αντικαθίστανται από άλλα τα οποία διατηρούνται στην ίδια διάταξη όπως και τα πρωτότυπά τους στο αρχικό κείμενο. Αν οι αντικαταστάτες παραμένουν οι ίδιοι σε όλο το κείμενο (κάθε γράμμα του αρχικού κειμένου αναπαρίσταται πάντοτε από το ίδιο σύμβολο-αντικαταστάτη) τότε το σύστημα ονομάζεται *μονοαλφαβητικό*. Αν το αρχικό κείμενο είναι σε κάποια φυσική γλώσσα, η κρυπτανάλυση είναι πάντοτε εφικτή βασιζόμενη στη στατιστική κατανομή των γραμμάτων. Στα *πολυαλφαβητικά* συστήματα αντικατάστασης κάθε γράμμα του αρχικού κειμένου μπορεί να έχει πολλούς αντικαταστάτες και κάθε φορά χρησιμοποιείται διαφορετικός αντικαταστάτης.

Στα συστήματα μετάθεσης (ή αναδιάταξης) τα γράμματα του αρχικού κειμένου αναδιατάσσονται. Αυτή η μέθοδος είναι υπερβολικά απλή, οπότε θα πρέπει να συνδυαστεί με κάποια άλλη ιδέα (μέθοδο παρεμβολής σκουπιδιών, …). Ένα παράδειγμα συστήματος που χρησιμοποιεί τη μέθοδο παρεμβολής σκουπιδιών δίνεται στο παράδειγμα 16.1 παρακάτω.

Μια άλλη κατηγοριοποίηση των κρυπτοσυστημάτων θα μπορούσε να είναι σε συστήματα αντικατάστασης *χωρίς συμφραζόμενα (context-free)* και σε συστήματα αντικατάστασης *με συμφραζόμενα (context-sensitive)* : Στα συστήματα χωρίς συμφραζόμενα κάθε γράμμα κωδικοποιείται ξεχωριστά ενώ σε εκείνα με συμφραζόμενα η κωδικοποίηση γίνεται ανά ομάδες (blocks).

Παράδειγμα 16.1. Μέθοδος Παρεμβολής Σκουπιδιών Σύστημα RICHELIEU

Αυτό το σύστημα χρησιμοποιεί τη μέθοδο “παρεμβολής σκουπιδιών”, και μπορεί να κρυπτογραφήσει ένα αρχικό κείμενο παράγοντας κρυπτοκείμενο που δείχνει πολύ αθώο …. Ο Richelieu χρησιμοποιούσε κομάτια χαρτονιού με τρύπες. Μόνο τα γράμματα που φαίνονται από τις τρύπες είναι σημαντικά. Για παράδειγμα, θεωρείστε ένα block 70 χαρακτήρων διατεταγμένων σε 7 γραμμές και 10 στήλες. Επίσης θεωρείστε ότι οι τρύπες είναι στις θέσεις:

$$(1,8),(2,9),(3,6),(4,5),(4,6),(5,1),(5,6),(5,7),(5,9),(6,2),(6,10),(7,9),(7,10)$$

	1	2	3	4	5	6	7	8	9	10
1								□		
2									□	
3						□				
4					□	□				
5	□					□	□		□	
6		□								□
7									□	□

Κρυπτοκείμενο:

I		L	O	V	E		Y	O	U
I		H	A	V	E		Y	O	U
D	E	E	P		U	N	D	E	R
M	Y		S	K	I	N		M	Y
L	O	V	E		L	A	S	T	S
F	O	R		E	V	E	R	I	N
H	Y	P	E	R	S	P	A	C	E

Το αρχικό κείμενο εδώ είναι YOU KILL AT ONCE, ενώ το κρυπτοκείμενο είναι αρκετά αθώο (άσχετο).

16.3.1 Μονοαλφαβητικά Συστήματα Αντικατάστασης

Ένα κρυπτοσύστημα ονομάζεται μονοαλφαβητικό αν κάθε γράμμα του αρχικού κειμένου αναπαρίσταται πάντοτε από το ίδιο σύμβολο-αντικαταστάτη (κάθε εμφάνιση ενός συμβόλου του αρχικού κειμένου κρυπτογραφείται με τον ίδιο πάντα αντικαταστάτη).

Παράδειγμα 16.2. Το Κρυπτοσύστημα του ΚΑΙΣΑΡΑ

Το κρυπτοσύστημα του Καίσαρα είναι από τα πρώτα κρυπτογραφικά σχήματα που χρησιμοποιήθηκαν. Είναι επίσης πολύ απλό, και μπορεί κανείς να το σπάσει πολύ εύκολα. Το σύστημα του Καίσαρα βασίζεται σε αντικαταστάσεις (μονοαλφαβητικό σύστημα αντικατάστασης): ολίσθηση κατά k θέσεις, δηλαδή κάθε γράμμα αντικαθίσταται με άλλο, προχωρώντας k θέσεις στο αλφάβητο modulo το μέγεθος του αλφαβήτου. ($k = 1, \ldots, 25$). Π.χ. για $k = 3$:

Τα γράμματα του αρχικού κειμένου:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Οι αντικαταστάτες του κρυπτοκειμένου:
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Για παράδειγμα το αρχικό κείμενο I LOVE MATH κρυπτογραφείται ως LORYH PDWK. Η μέθοδος κρυπτογράφησης E_k είναι ολίσθηση μπροστά κατά k βήματα στο αλφάβητο, και η μέθοδος αποκρυπτογράφησης είναι ολίσθηση πίσω κατά k βήματα στο αλφάβητο. Παρακάτω δίνονται κάποιες προφανείς ιδιότητες των E_k και D_k :

$$E_i \circ D_j = D_j \circ E_i \text{ (αντιμεταθετική ιδιότητα)}$$

$$D_k = E_{26-k}\ ,\ D_k \circ E_k = D_0 = E_0 = D_{26} = E_{26}.$$

Αν το αρχικό κείμενο ανήκει σε μια γνωστή φυσική γλώσσα, η κρυπτανάλυση αυτού του συστήματος είναι πολύ εύκολη: από τη στιγμή που ο συνολικός αριθμός των δυνατών κλειδιών είναι αρκετά μικρός (25) μπορεί κανείς απλά να τα δοκιμάσει όλα σε ένα μικρό μέρος του κρυπτοκειμένου και να δει ποιο από όλα οδηγεί σε αρχικό κείμενο που έχει νόημα. Επίσης, όπως και όλα τα μονοαλφαβητικά συστήματα αντικατάστασης, το σύστημα του Καίσαρα μπορεί να το σπάσει κανείς υπολογίζοντας τις συχνότητες εμφάνισης των γραμμάτων.

□

Παράδειγμα 16.3. Μια παραλλαγή: Το σύστημα του Καίσαρα με λέξη-κλειδί (KEYWORD-CAESAR system)

Για ένα Καισαρικό κρυπτοσύστημα μπορούμε να χρησιμοποιήσουμε οποιαδήποτε αντιμετάθεση του χρησιμοποιούμενου αλφαβήτου, προκειμένου να ορίσουμε τους αντικαταστάτες για το κάθε γράμμα του αλφαβήτου. Το κλειδί για το συγκεκριμένο σύστημα είναι η αντιμετάθεση που χρησιμοποιείται. Το σύστημα του Καίσαρα με λέξη κλειδί παράγει μια συγκεκριμένη αντιμετάθεση χρησιμοποιώντας έναν αριθμό (κλειδί) και μια λέξη ή μια μικρή φράση (λέξη-κλειδί): Επιλέγουμε έναν αριθμό k τέτοιον ώστε $0 \leq k \leq 26$ (=πληθάριθμος του αλφαβήτου του απλού κειμένου) και μια λέξη-κλειδί (ή φράση-κλειδί) στην οποία όλα τα γράμματα είναι διαφορετικά. Για παράδειγμα, θεωρείστε $k = 7$, και τη λέξη-κλειδί "TEN FOUR". Γράψτε τη λέξη-κλεδί κάτω από το αλφάβητο, ξεκινώντας από το k-οστό γράμμα:

```
0             7                                   25
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
              T E N F O U R
```

Συμπληρώστε τη δεύτερη γραμμή με τα υπόλοιπα γράμματα σε αλφαβητική σειρά, μετά τη λέξη-κλειδί:

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
P S V W X Y Z T E N F O U R A B C D G H I J K L M Q
```

Δεν είναι απαραίτητο τα γράμματα στη λέξη-κλειδί να είναι διαφορετικά: απλά θα μπορούσε να γραφεί η λέξη-κλειδί χωρίς επαναλήψεις. Ο αριθμός των κλειδιών σε ένα τέτοιο σύστημα είναι μεγάλος (υπάρχουν 26! αντιμεταθέσεις για το Αγγλικό αλφάβητο), οπότε η κρυπτανάλυση θα πρέπει να βασιστεί στη μέτρηση συχνοτήτων. □

Ένας (απλός) τρόπος άμυνας απέναντι στην κρυπτανάλυση τη βασισμένη σε μετρήσεις συχνότητας, είναι το κρυπτοσύστημα με ομόφωνα (HOMOPHONES): Τα γράμματα του αρχικού κειμένου έχουν πολλούς αντικαταστάτες (λέγονται *ομόφωνα-homophones*) - ο αριθμός των αντικαταστατών είναι ανάλογος της συχνότητας με την οποία εμφανίζεται το γράμμα στη γλώσσα του απλού κειμένου. Σε αυτό το σύστημα προκειμένου να κρυπτογραφήσουμε την εμφάνιση κάποιου γράμματος επιλέγουμε τυχαία έναν από τους αντικαταστάτες. Το σύστημα αυτό δεν είναι μονοαλφαβητικό, και επιπλέον, η μέθοδος κρυπτογράφησης δεν είναι (ντετερμινιστική) συνάρτηση. Σημειώνουμε ότι ένα απλό κείμενο είναι δυνατόν να αντιστοιχεί σε αρκετά διαφορετικά

κρυπτοκείμενα, αντιθέτως ένα κρυπτοκείμενο αντιστοιχεί μόνο σε ένα απλό κείμενο. Χρησιμοποιώντας την παραπάνω μέθοδο, μπορούμε να δούμε ότι κάθε σύμβολο στο κρυπτοκείμενο εμφανίζεται με την ίδια συχνότητα. Η κρυπτανάλυση του συγκεκριμένου συστήματος μπορεί να βασιστεί σε στατιστικές κατανομές ζευγαριών ή τριάδων γραμμάτων (στη γλώσσα του απλού κειμένου).

16.3.2 Πολυαλφαβητικά Συστήματα Αντικατάστασης

Αν σε ένα κρυπτοσύστημα, κάθε (διατεταγμένο) ζευγάρι γραμμάτων (ή block n γραμμάτων — n-γράμματο) του αλφαβήτου του απλού κειμένου κωδικοποιείται πάντοτε κατά τον ίδιο τρόπο (με τον ίδιο αντικαταστάτη) τότε το σύστημα εξακολουθεί να είναι μονοαλφαβητικό, και συνήθως λέγεται *μονοαλφαβητικό με την ευρεία έννοια (monoalphabetic in a wider sense)*. Στα πολυαλφαβητικά κρυπτοσυστήματα αντικατάστασης, ένα γράμμα δεν αντικαθίσταται από το ίδιο σύμβολο παντού στο κείμενο: η χρήση των αντικαταστατών ποικίλει στα διάφορα μέρη του απλού κειμένου, και δεν είναι καν μονοαλφαβητική με την ευρεία έννοια (η αντικατάσταση του κάθε γράμματος του κειμένου γίνεται *με συμφραζόμενα*. Παρατηρήστε ότι τα μονολφαβητικά συστήματα με την ευρεία έννοια είναι επίσης με συμφραζόμενα).

Η γερμανική μηχανή Αίνιγμα θεωρείται σύστημα πολυαλφαβητικής αντικατάστασης (μετά από κάθε γράμμα του κειμένου, τα γρανάζια γυρίζουν, δίνοντας ένα νέο πρότυπο κρυπτογράφησης).

Ο κώδικας αντικατάστασης 2-γραμμάτων PLAYFAIR (Βαρώνος Playfair του Αγ. Ανδρέα)

Το κρυπτοσύστημα Playfair βασίζεται στο Αγγλικό αλφάβητο, και είναι μονοαλφαβητικό σύστημα με την ευρεία έννοια.

Διατάσσουμε τα γράμματα του Αγγλικού αλφαβήτου, παραλείποντας το J (το J και το I θεωρούνται σαν το ίδιο γράμμα) σε έναν πίνακα 5×5 (που λέγεται τετράγωνο Playfair), με κάποιο τυχαίο τρόπο. Συνήθως το τετράγωνο Playfair δημιουργείται βασισμένο σε μια λέξη-κλειδί (ή φράση): τα γράμματα της λέξης κλειδί (οι επαναλήψεις διαγράφονται) τοποθετούνται κατά σειρές, ακολουθούμενα από τα υπόλοιπα γράμματα σε αλφαβητική σειρά. (Οι λέξεις-κλειδιά χρησιμοποιούνται προκειμένου να γίνει η διαχείρηση του κλειδιού ευκολότερη) Για παράδειγμα, η λέξη-κλειδί PLAYFAIR δίνει τον παρακάτω πίνακα:

P	L	A	Y	F
I	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Χωρίζουμε το αρχικό κείμενο σε blocks που αποτελούνται από δύο γράμματα το καθένα (2-γράμματα). Δεν πρέπει κανένα block να περιέχει δύο φορές το ίδιο γράμμα: οποτεδήποτε συμβαίνει αυτό, παρεμβάλουμε (μεταξύ των δύο γραμμάτων στο αρχικό κείμενο) ένα *μηδενικό χαρακτήρα* (συνήθως το Q). Επίσης το απλό κείμενο πρέπει να περιέχει άρτιο αριθμό γραμμάτων (διαφορετικά βάζουμε ένα μηδενικό χαρακτήρα στο τέλος του). Οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης λειτουργούν στα 2-γράμματα όπως φαίνεται παρακάτω:

Κρυπτογράφηση:

Αν τα δύο γράμματα του block δεν είναι στην ίδια γραμμή ή στήλη του τετραγώνου Playfair, τότε κωδικοποιούμε χρησιμοποιώντας τις άλλες δύο γωνίες του ορθογωνίου που ορίζεται από τα δύο γράμματα του block. Για παράδειγμα, χρησιμοποιώντας το παραπάνω τετράγωνο Playfair, το 2-γραμμα AD ορίζει το ορθογώνιο AFBD και κρυπτογραφείται ως FB.

Αν τα δύο γράμματα του block είναι στην ίδια γραμμή (στήλη), επιλέγουμε (κυκλικά) τα γειτονικά γράμματα δεξιά (κάτω) για κάθε γράμμα του block. Έτσι, το RC κωδικοποιείται με το BD, το AW με το BA, το UV με το VW.

Με αυτή τη μέθοδο το αρχικό κείμενο MATHEMATICS χωρίζεται σε 2-γράμματα ως MA TH EM AT IC SQ και κρυπτογραφείται: HF QM GE FQ RD TS.

Η μέθοδος αποκρυπτογράφησης είναι προφανής: αφού το PLAYFAIR είναι ένα κλασικό διπλής-κατεύθυνσης κρυπτοσύστημα η αποκρυπτογράφηση προκύπτει (εύκολα) από τη μέθοδο κρυπτογράφησης.

Η κρυπτανάλυση αυτού του συστήματος μπορεί επίσης να βασιστεί στη μέθοδο της μέτρησης συχνοτήτων (όπως και για όλα τα μονοαλφαβητικά συστήματα αντικατάστασης), αλλά η ανάλυση είναι πιο πολύπλοκή καθώς η κρυπτογράφηση βασίζεται σε 2-γράμματα, και όχι σε απλά γράμματα. □

Τα πολυαλφαβητικά συστήματα παρέχουν μια πολύ καλή άμυνα εναντίον της μέτρησης συχνοτήτων διότι κάθε γράμμα δεν αναπαρίσταται με το ίδιο σύμβολο παντού στο απλό κείμενο.

Κρυπτοσύστημα VIGENÉRE (Blaise de Vigenére 1523-1596)

Το σύστημα του Vigenére είναι από τα πιο παλιά και τα πιο γνωστά πολυαλφαβητικά κρυπτοσυστήματα (στην πραγματικότητα ο κώδικας Αίνιγμα και ο κώδικας Vernam είναι Vigenére συστήματα). Αρχικά αντιστοιχίζουμε σε κάθε γράμμα του αλφαβήτου έναν αριθμό $(A-0, B-1, \ldots, Z-25)$. Το VIGENÉRE μπορεί να θεωρηθεί ένα σύστημα του Καίσαρα στο οποίο το κλειδί αλλάζει από βήμα σε βήμα. Το κλειδί στο σύστημα VIGENÉRE είναι ένα διάνυσμα $k = (k_0, k_1, \ldots, k_{r-1})$. Αυτό το διάνυσμα είναι η λέξη-κλειδί, και μπορεί να είναι οποιαδήποτε λέξη ή φράση (επαναλήψεις γραμμάτων επιτρέπονται). Ο αριθμός r λέγεται περίοδος του συστήματος. Το αρχικό κείμενο διαιρείται σε blocks μεγέθους r και κάθε block κρυπτογραφείται χρησιμοποιώντας τη λέξη-κλειδί ως εξής: γράφουμε τη λέξη-κλειδί κάτω από το block του αρχικού κειμένου και κρυπτογραφούμε κάθε γράμμα του κειμένου χρησιμοποιώντας ένα σύστημα του Καίσαρα με το k να ισούται με τον αριθμό που αντιστοιχεί στο γράμμα της λέξης-κλειδί που είναι γραμμένη από κάτω. Έτσι η αντικατάσταση VIGENÉRE για κάθε block του αρχικού κειμένου ορίζεται ως:

$$f : (x_0, \ldots, x_{r-1}) \to (x_0 + k_0, \ldots, x_{r-1} + k_{r-1})$$

Η κρυπτανάλυσή του γίνεται με τον ίδιο ακριβώς τρόπο με τον οποίο γίνεται και η κρυπτανάλυση του συστήματος του Καίσαρα. Τα γράμματα ανά r έχουν κρυπτογραφηθεί με τον ίδιο αριθμό ολίσθησης. Αν όμως δεν γνωρίζουμε το μήκος r της λέξης-κλειδί θα πρέπει να το βρούμε. Αυτό γίνεται δύσκολα, με παρατήρηση των επαναλήψεων ίδιων ακολουθιών γραμμάτων σε διαφορετικά σημεία του κειμένου. Αν π.χ. επαλαμβάνεται μια λέξη σε δύο σημεία με απόσταση m

μεταξύ τους, τότε ίσως πρόκειται για την ίδια λέξη που κρυπτογραφήθηκε με το ίδιο μέρος του κλειδιού. Τότε το m είναι πολλαπλάσιο του r.

Οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης μπορούν να εκτελεστούν και χωρίς υπολογιστή χρησιμοποιώντας έναν πίνακα παρόμοιο με τον παρακάτω, στον οποίο κάθε στήλη μπορεί να θεωρηθεί ως ένα σύστημα του Καίσαρα. Για να χρησιμοποιήσουμε αυτόν τον πίνακα διαβάζουμε το κείμενο από την πρώτη στήλη, το κλειδί από την πρώτη γραμμή και το κρυπτοκείμενο είναι το γράμμα που βρίσκεται στην τομή τους. Για την αποκρυπτογράφηση, βρίσκουμε το γράμμα του κρυπτοκειμένου στη στήλη που υποδεικνύεται από το κλειδί και διαβάζουμε το αντίστοιχο γράμμα του αρχικού κειμένου από την πρώτη στήλη της γραμμής στην οποία βρίσκεται το γράμμα του κρυπτοκειμένου. (Σημειώνεται ότι ο ρόλος των γραμμών και των στηλών μπορεί να εναλλαχθεί)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Η κρυπτογράφηση του αρχικού κειμένου χρειάζεται μια λέξη-κλειδί μήκους r η οποία επαναλαμβάνεται για να καλύψει όλο το αρχικό κείμενο. Τέτοια πολυαλφαβητικά συστήματα, όπου τα αλφάβητα των αντικαταστατών επαναλαμβάνονται περιοδικά συνήθως ονομάζονται *περιοδικά*.

Αν γνωρίζουμε την περίοδο κάποιου περιοδικού πολυαλφαβητικού συστήματος, τότε η κρυπτανάλυσή του μπορεί να αναχθεί στην κρυπτανάλυση ενός μονοαλφαβητικού συστήματος: Θεωρούμε ότι η περιοδός είναι r. Διατάσσουμε τα γράμματα του κρυπτοκειμένου σε γραμμές με r στήλες σε κάθε γραμμή (γράφουμε r γράμματα σε κάθε γραμμή). Δύο εμφανίσεις του ίδιου γράμματος στην ίδια στήλη αντιπροσωπεύουν το ίδιο αρχικό γράμμα. Οπότε μπορούμε να αποκρυπτογραφήσουμε κάθε στήλη με μέτρηση συχνοτήτων.

Αν η περίοδος που χρησιμοποιείται σε ένα περιοδικό σύστημα τύπου VIGENÉRE είναι άγνωστη, μπορεί (ίσως) να βρεθεί με την *μέθοδο του Kasiski* (F.W. Kasiski, 1860): Αυτή η μέθοδος υπολογίζει την περίοδο ψάχνοντας τις εμφανίσεις της ίδιας λέξης στο κρυπτοκείμενο. Υποθέτουμε ότι μια συγκεκριμένη λέξη εμφανίζεται δύο φορές στο κρυπτοκείμενο, και ότι μεσολαβούν m γράμματα μεταξύ των εμφανίσεων αυτών (δηλαδή από την αρχή της πρώτης μέχρι την αρχή της δεύτερης). Αυτό μπορεί να οφείλεται στο ότι οι δύο εμφανίσεις αντιστοιχούν στο ίδιο κομμάτι του αρχικού κειμένου, που έχει κρυπτογραφηθεί ξεκινώντας από την ίδια θέση του κλειδιού. Σε

αυτήν την περίπτωση, η απόσταση m μεταξύ των δύο εμφανίσεων στο κρυπτοκείμενο θα πρέπει να είναι πολλαπλάσιο του μήκους του κλειδιού. Αν βρεθούν αρκετές τέτοιες διπλές εμφανίσεις στο κρυπτοκείμενο, μπορούμε να κάνουμε μια καλή εκτίμηση για το μήκος του κλειδιού.

Το κρυπτοσύστημα AUTOCLAVE (G. Cardano[2])

Το σύστημα AUTOCLAVE είναι μια παραλλαγή του γενικού συστήματος VIGENÉRE όπου το αρχικό κείμενο χρησιμοποιείται επίσης και ως κλειδί κρυπτογράφησης, μετά από κάποια ολίσθηση. Συνήθως, μια λέξη-κλειδί χρησιμοποιείται στην αρχή του κειμένου (η οποία δίνει την απαιτούμενη ολίσθηση). Για παράδειγμα, το αρχικό κείμενο EVERYTHING IS MATHEMATICS, χρησιμοποιώντας τη λέξη-κλειδί CRYPTO θα κρυπτογραφηθεί ως εξής:

Αρχικό κείμενο	E	V	E	R	Y	T	H	I	N	G	I	S	M	A	T	H	E	M	A	T	I	C	S
Κλειδί	C	R	Y	P	T	O	E	V	E	R	Y	T	H	I	N	G	I	S	M	A	T	H	E
Κρυπτοκείμενο	G	M	C	G	R	H	L	D	R	X	G	L	T	I	G	N	M	E	M	T	B	J	W

Σε μια παραλλαγή του AUTOCLAVE, το κρυπτοκείμενο που δημιουργείται με τον παραπάνω τρόπο, χρησιμοποιείται ως κλειδί κρυπτογράφησης μετά τη λέξη κλειδί κ.ο.κ. Για παράδειγμα:

Αρχικό κείμενο	E	V	E	R	Y	T	H	I	N	G	I	S	M	A	T	H	E	M	A	T	I	C	S
Κλειδί	C	R	Y	P	T	O	G	M	C	G	R	H	N	U	P	M	Z	Z	Z	U	I	T	D
Κρυπτοκείμενο	G	M	C	G	R	H	N	U	P	M	Z	Z	Z	U	I	T	D	L	Z	N	Q	V	V

Η κρυπτανάλυση του συστήματος AUTOCLAVE είναι σχετικά απλή: Χρειάζεται μόνο να μαντέψουμε το μήκος της λέξης-κλειδί, έστω n. Στο παραπάνω κρυπτοκείμενο, αν γνωρίζουμε το μήκος της λέξης κλειδί (= 6), τότε έχουμε το εξής σενάριο:

Κρυπτοκείμενο	G	M	C	G	R	H	N	U	P	M	Z	Z	Z	U	I	T	D	L	Z	N	Q	V	V
Κλειδί						G	M	C	G	R	H	N	U	P	M	Z	Z	Z	U	I	T	D	
Αρχικό κείμενο						H	I	N	G	I	S	M	A	T	H	E	M	A	T	I	C	S	

Η κρυπτανάλυση του προηγούμενου συστήματος AUTOCLAVE έχει ως εξής: Αρχικά χρησιμοποιούμε τη μέθοδο Kasiski για να καθορίσουμε το μήκος του κλειδιού (την *περίοδο*). Η μέθοδος του Kasiski δεν είναι τόσο καλή για τα συστήματα AUTOCLAVE όσο είναι για το σύστημα VIGENÉRE, αλλά συνήθως είναι αρκετά καλή. Για παράδειγμα, ας υποθέσουμε ότι το αρχικό κείμενο περιέχει δύο εμφανίσεις της λέξη THE και ότι η απόσταση μεταξύ αυτών των δύο εμφανίσεων είναι δύο φορές η περίοδος. Τότε κάποια ακολουθία τριών γραμμάτων, έστω AID θα βρίσκεται στο ενδιάμεσο των δύο εμφανίσεων. Κατά τη διαδικασία κρυπτογράφησης θα έχουμε:

Αρχικό κείμενο	…	T	H	E	…	A	I	D	...	T	H	E ...
Κλειδί	...				...	T	H	E	...	A	I	D ...
Κρυπτοκείμενο	...				...	T	P	H	...	T	P	H ...

[2]G. Cardano(1501-1576), Ιταλός Μαθηματικός, γιατρός και φιλόσοφος - Τύποι επίλυσης εξισώσεων τρίτου και τετάρτου βαθμού

οπότε, συναντάμε το ΤΡΗ δύο φορές στο κρυπτοκείμενο και η απόσταση μεταξύ των δύο εμφανίσεων δίνει την περίοδο του συστήματος. Από τη στιγμή που είναι γνωστή η περίοδος, βρίσκουμε τη λέξη-κλειδί με εξαντλητικό ψάξιμο βασισμένο στη μέτρηση συχνοτήτων του κάθε γράμματος.

Υπάρχει επίσης μια παραλλαγή του κώδικα PLAYFAIR, το ΠΕΡΙΟΔΙΚΟ PLAYFAIR, το οποίο είναι πολυαλφαβητικό (και εξαρτάται από τα συμφραζόμενα, όπως και το μονοαλφαβητικό PLAYFAIR): Αντί για ένα τετράγωνο PLAYFAIR, χρησιμοποιούμε περισσότερα τετράγωνα, έστω k. Το πρώτο γράμμα του αρχικού κειμένου, κρυπτογραφείται σύμφωνα με το πρώτο τετράγωνο, το δεύτερο ώς k-οστό γράμμα με το δεύτερο ως k-οστό τετράγωνο αντίστοιχα και το $k+1$-οστό γράμμα με το πρώτο τετράγωνο κ.ο.κ.

Ο κώδικας Vernam ή Μπλοκάκι μιας Χρήσης (Vernam, 1917)

Το μπλοκάκι (για το κλειδί) μιας χρήσης είναι ένα τέλειο κρυπτογραφικό σύστημα που παρέχει απόλυτη μυστικότητα με την έννοια ότι το κρυπτοκείμενο δεν περικλείει καμία απολύτως πληροφορία σχετικά με το αρχικό κείμενο ή το σύστημα. Ο κρυπταναλυτής έχει την ίδια πληροφορία για το αρχικό κείμενο ή το σύστημα είτε γνωρίζοντας το κρυπτοκείμενο είτε όχι. Μάλιστα, αυτό ισχύει ακόμη και αν γνωρίζει ένα μέρος του αρχικού μηνύματος.

Το μπλοκάκι μιας χρήσης είναι ένα κρυπτοσύστημα μυστικού κλειδιού (κλασικό) όπου το κλειδί έχει το ίδιο μήκος με το κείμενο προς κρυπτογράφηση. Επιπλέον, το κλειδί το χρησιμοποιούμε μόνο μια φορά και μετά το "πετούμε", δεν το ξαναχρησιμοποιούμε.

Το αρχικό κείμενο M αναπαριστάται ως δυαδική ακολουθία, όπως επίσης και το κλειδί K. Το κρυπτοκείμενο C προκύπτει από τη αποκλειστική διάζευξη ανά bit (XOR) (ή πρόσθεση modulo 2) του αρχικού κειμένου με το κλειδί:

$C = M \oplus K$. Η αποκρυπτογράφηση δίνεται από το $M = C \oplus K$.

Αποδεικνύεται ότι είναι αδύνατο για τον κρυπταναλυτή να σπάσει τον κώδικα που χρησιμοποιεί μπλοκάκι μιας χρήσης: Οποιοδήποτε κρυπτοκείμενο C δεν αποκαλύπτει καμία πληροφορία για το αρχικό κείμενο M αφού κάθε μήνυμα M θα μπορούσε να παραγάγει το C, αν το κλειδί K ήταν ίσο με $K = C \oplus M$.

Η κρυπτογράφηση με μπλοκάκι μιας χρήσης είναι αποδεδειγμένα ασφαλής με πληροφοριοθεωρητική έννοια, αφού ο υποκλοπέας δεν έχει ποτέ αρκετή πληροφορία για να αποκρυπτογραφήσει το κρυπτοκείμενο και καμμία ποσότητα υπολογιστικής δύναμης δεν μπορεί να τον βοηθήσει.

Από την άλλη πλευρά, το μπλοκάκι μιας χρήσης δεν είναι πρακτικό αφού ένα μεγάλο κλειδί πρέπει να δημιουργηθεί, να διανεμηθεί και να αποθηκευτεί.

Τα σύγχρονα κρυπτοσυστήματα χρησιμοποιούν σχετικά μικρά κλειδιά (56 - 1000 bits) και (επιδιώκουν να) είναι ασφαλή με την υπολογιστική έννοια, εννοώντας ότι η κρυπτανάλυσή τους είναι υπολογιστικά απρόσιτη (ανέφικτη).

16.4 Κρυπτοσυστήματα Πακέτου (Block Ciphers)

16.4.1 Τα κρυπτοσυστήματα DES (Data Encryption Standard) και AES (Adavanced Encrytpion Standard)

Το 1972 το αμερικάνικο NBS (National Bureau of Standards) , νυν NIST (National Institute of Standards and Technology), ξεκίνησε ένα πρόγραμμα για την προστασία δεδομένων, στου οποίου τα πλαίσια αναζήτησε έναν αλγόριθμο κρυπτογράφησης που θα λειτουργούσε ως πρότυπο. Το 1974, η IBM πρότεινε ένα κρυπτοσύστημα βασισμένο στον αλγόριθμο «Lusifer», το οποίο σταδιακά εξελίχθηκε στο DES (Data Encryption Standard).

Το DES τέθηκε σε ισχύ το 1977 από το αμερικάνικο Υπουργείο Εμπορίου ως πρότυπο για την προστασία *ευαίσθητων αλλά όχι απόρρητων* δεδομένων. Μετά το NBS, πολλοί άλλοι οργανισμοί υιοθέτησαν το DES. Ανάμεσά τους το ANSI (American National Standards Institute) και η American Bankers Association.

Το DES είναι ένα κρυπτοσύστημα πακέτου (block chipher) διαστάσεων 64×56, του οποίου κύριο δομικό στοιχείο είναι ένα Feistel δίκτυο διαστάσεων $64 \times 48 \times 16$. Παρά το μεγάλο χρονικό διάστημα στο οποίο παρέμεινε το ευρύτερα διαδεδομένο κρυπτοσύστημα παγκοσμίως, το DES αποδείχθηκε ιδιαίτερα ανθεκτικό στις κρυπταναλυτικές επιθέσεις. Οι πρώτες επιθέσεις που είχαν ουσιαστικά καλύτερο αποτέλεσμα από την *εξαντλητική αναζήτηση κλειδιού* αναπτύχθηκαν μέσα στη δεκαετία του '90.

Το DES δεν είναι πληροφοριοθεωρητικά ασφαλές αλλά η κρυπτανάλυσή του είναι υπολογιστικά απρόσιτη.

Κρυπτογράφηση: Χωρίζουμε το αρχικό κείμενο σε κομμάτια των 64 bits, και σε κάθε κομμάτι εφαρμόζουμε μια συγκεκριμένη μετάθεση των bits του αρχικού κειμένου (αυτή η μετάθεση δεν έχει προφανή κρυπτογραφική σημασία). Το κείμενο που προκύπτει χωρίζεται σε αριστερά και δεξιά κομμάτια των 32 bits L και R αντίστοιχα, τα οποία κρυπτογραφούνται με τις εξής πράξεις ($i = 1, \ldots, 16$)

$$
\begin{aligned}
L_i &= R_{i-1} \\
R_i &= L_{i-1} \oplus f(R_{i-1}, K_{i-1})
\end{aligned}
$$

Η συνάρτηση f ορίζεται με τη χρήση συναρτήσεων αντικατάστασης (ή *κουτιών* S), οι οποίες απεικονίζουν εισόδους των 6 bits σε εξόδους των 4 bits. Τα 16 κλειδιά K_i προκύπτουν από το αρχικό κλειδί K με κατάλληλες μεταθέσεις και επιλογή των ψηφίων του.

Το DES είναι αντιστρέψιμο ανεξάρτητα από τον ορισμό της f.

Ο αλγόριθμος του DES είναι πολύ γρήγορος, ιδίως με εξειδικευμένο hardware. Από την άλλη πλευρά, η κρυπτανάλυση μας οδηγεί σε διάφορα μη-γραμμικά συστήματα εξισώσεων και τα προβλήματα που προκύπτουν είναι το λιγότερο NP-πλήρη.

Το 1993 οι Biham και Shamir ανέπτυξαν μια επίθεση με επιλεγμένα απλά κείμενα γνωστή ως *διαφορική κρυπτανάλυση* ενώ το 1994 ο Matsui εισήγαγε την *γραμμική κρυπτανάλυση*, μια επίθεση με γνωστά απλά κείμενα. Τόσο η διαφορική όσο και η γραμμική κρυπτανάλυση αποτελούν

ιδιαίτερα σημαντικές κρυπταναλυτικές τεχνικές, η πρακτική τους ωστόσο επίδραση στην ασφάλεια του DES είναι μικρή αφού απαιτούν έναν τεράστιο αριθμό επιλεγμένων ή γνωστών απλών κειμένων αντίστοιχα. Το καθοριστικό ρήγμα στην ασφάλεια του DES προέρχεται από το μικρό μήκος του κλειδιού που χρησιμοποιείται. Για τα σημερινά τεχνολογικά δεδομένα το μήκος κλειδιού 56 bit παρέχει πράγματι μικρή ασφάλεια απέναντι στην τετριμμένη επίθεση της εξαντλητικής αναζήτησης. Ενδεικτικά αναφέρουμε ότι το 1998 η ειδικά κατασκευασμένη μηχανή Deep Crack της Electronic Frontier Foundation έσπασε το DES σε 56 ώρες έχοντας ψάξει το 25% του χώρου των κλειδιών.

Ως προσωρινή λύση για ασφαλέστερη κρυπτογράφηση είχε ήδη προταθεί από το 1993 το Triple-DES, το οποίο αν και είναι πράγματι ασφαλέστερο του DES, είναι και τρεις φορές πιο αργό.

Τον Ιανουάριο του 1997 το NIST ανακοίνωσε την πρόθεση για την ανάπτυξη ενός νέου κρυπτογραφικού προτύπου, του AES (Advanced Encryption Standard), που θα αντικαθιστούσε το DES. Τον Σεπτέμβριο του 1997 ανακοινώθηκε η έναρξη ανοιχτού διαγωνισμού. Το NIST δεν θα προχωρούσε σε αξιολόγηση της ασφάλειας και της αποδοτικότητας των υποψηφίων κρυπτοσυστημάτων, αλλά κάλεσε την κρυπτολογική κοινότητα να πραγματοποιήσει επιθέσεις. Τα σχετικά αποτελέσματα θα ανακοινώνονταν σε μια σειρά συνεδρίων.

Η επιλογή έγινε τόσο με βάση την ασφάλεια — αντοχή στις επιθέσεις που πραγματοποιήθηκαν, αλλά και θεωρητική άμυνα απέναντι σε μεθόδους γραμμικής και διαφορικής κρυπτανάλυσης — όσο και με βάση την ταχύτητα, την απλότητα και την ευελιξία του Rijndael. Το AES τέθηκε σε ισχύ στις 26 Μαΐου 2002 από το αμερικάνικο Υπουργείο Εμπορίου.

16.5 Συστήματα δημοσίου κλειδιού

Η ιδέα της κρυπτογραφίας δημοσίου κλειδιού πρωτοπαρουσιάστηκε από τους Diffie και Hellman σε μια εργασία που δημοσιεύτηκε το 1976 ([2]). Η κρυπτογραφία δημόσιου κλειδιού παρουσιάστηκε σχετικά αργά (αν σκεφτούμε ότι είναι μια σχετικά απλή ιδέα και η ιστορία της κρυπτογραφίας πολύ μεγάλη), βασικά διότι οι περισσότερες θεμελιώδεις έννοιες συνδέονται ιδιαίτερα με τη θεωρία πολυπλοκότητας, η οποία αναπτύχθηκε σχετικά πρόσφατα.

Παράδειγμα 16.4. Αυτό το παράδειγμα δίνει μια πολύ γενική ιδέα της κρυπτογραφίας δημοσίου κλειδιού. Σκεφθείτε τον τηλεφωνικό κατάλογο. Είναι εύκολο να βρείτε το νούμερο του τηλεφώνου ενός ατόμου, αλλά μάλλον δύσκολο να βρείτε το πρόσωπο που έχει ένα συγκεκριμένο τηλεφωνικό νούμερο. Αυτό δίνει την ιδέα της συνάρτησης μονής κατεύθυνσης: Είναι εύκολο να υπολογίσει κάποιος τη συνάρτηση αλλά ο αντίστροφος υπολογισμός είναι πολύ δύσκολος (απρόσιτος). Σε αυτό το παράδειγμα ο τηλεφωνικός κατάλογος είναι το κλειδί κρυπτογράφησης που μπορεί να δημοσιευτεί με ασφάλεια (δημόσιο κλειδί). Το αρχικό κείμενο μπορεί να κρυπτογραφηθεί ως εξής: Αντικαθιστούμε κάθε γράμμα του αρχικού κειμένου με το νούμερο τηλεφώνου ενός ατόμου που το όνομά του αρχίζει με αυτό το γράμμα (επιλεγμένου τυχαία από τον κατάλογο). Το σύστημα είναι πολυαλφαβητικό αφού είναι εξαιρετικά απίθανο δύο εμφανίσεις του ίδιου γράμματος να κρυπτογραφηθούν με τον ίδιο τρόπο. Σημειώστε επίσης ότι η κρυπτογράφηση είναι μη ντετερμινιστική. Προκειμένου να αποκρυπτογραφήσουμε το κρυπτοκείμενο χρειάζεται να επεξεργαστούμε έναν κατάλογο ονομάτων και τους αντίστοιχους αριθμούς τηλεφώνων, ταξινομημένα με βάση τους αριθμούς τηλεφώνων (inverse catalog-index). Αυτός ο

αντίστροφος κατάλογος είναι το κλειδί αποκρυπτογράφησης (ιδιωτικό κλειδί). □

16.5.1 Γενικά

Η κρυπτογραφία δημοσίου κλειδιού βασίζεται στην ιδέα των *συναρτήσεων μονής-κατεύθυνσης*. Μία συνάρτηση $f(x)$ ονομάζεται μονής-κατεύθυνσης αν είναι εύκολο να υπολογίσουμε το $f(x)$ από το x (εύκολο = σε χαμηλό πολυωνυμικό χρόνο, προτιμότερα γραμμικό), ενώ ο αντίστροφος υπολογισμός δηλαδή του x από το $f(x)$ είναι απρόσιτος. Ένα πρόβλημα λέγεται συνήθως *απρόσιτο* αν δεν υπάρχει γνωστός πολυωνυμικός αλγόριθμος που να το λύνει, και *προσιτό* εάν υπάρχει τέτοιος αλγόριθμος (τότε λέμε ότι το πρόβλημα ανήκει στην κλάση P). Σημειώστε ότι απρόσιτα συνήθως θεωρούνται τα προβλήματα που είναι τουλάχιστον τόσο δύσκολα όσο και τα δυσκολότερα προβλήματα της κλάσης NP. Η χρήση των συναρτήσεων μονής-κατεύθυνσης προσφέρει στα κρυπτοσυστήματα δημοσίου κλειδιού την ιδιότητα: όταν γνωρίζουμε μόνο το κλειδί κρυπτογράφησης δεν μπορούμε να το χρησιμοποιήσουμε για να βρούμε το κλειδί αποκρυπτογράφησης χωρίς να χρειαστεί ένας πολύ μεγάλος υπολογισμός.

Ο ορισμός των συναρτήσεων μονής-κατεύθυνσης που δόθηκε παραπάνω, δεν είναι ακριβής από μαθηματική σκοπιά. Η έννοια του "απρόσιτου" (πρακτικά μη υπολογίσιμου) είναι στενά συνδεδεμένη με την τρέχουσα διαθέσιμη υπολογιστική δύναμη: είναι ουσιαστικά μια εμπειρική έννοια που εξαρτάται από την εξέλιξη της τεχνολογίας των υπολογιστών (π.χ. τεχνικές μαζικά παράλληλης επεξεργασίας). Έτσι, μια συνάρτηση που σήμερα θεωρείται ως ασφαλής συνάρτηση μονής-κατεύθυνσης μπορεί να χάσει αυτή της την ιδιότητα σε μερικές δεκαετίες.

Προκειμένου να *αποδείξουμε* ότι ένα κρυπτοσύστημα είναι σύστημα δημοσίου κλειδιού (δηλαδή ότι μια συνάρτηση είναι μονής-κατεύθυνσης) θα πρέπει να αποδείξουμε μαθηματικά ότι υπάρχει ένα μη τετριμένο κάτω όριο στο υπολογιστικό έργο που απαιτείται για την υλοποίηση ενός αλγορίθμου αποκρυπτογράφησης με άγνωστο το κλειδί αποκρυπτογράφησης. Ακόμη και για τα καλύτερα γνωστά συστήματα δημοσίου κλειδιού και τις συναρτήσεις που χρησιμοποιούν, δεν έχει αποδειχτεί ότι υπάρχει κάποιο τέτοιο κάτω όριο. Έτσι, τα περισσότερα κρυπτοσυστήματα δημοσίου κλειδιού που χρησιμοποιούνται σήμερα δεν είναι *αποδεδειγμένα* δημοσίου κλειδιού (απρόσιτα): είναι πάντα πιθανό ένας ικανός κρυπταναλυτής να τα σπάσει.

Στην κρυπτογραφία δημοσίου κλειδιού υπάρχουν δύο κλειδιά: το κλειδί κρυπτογράφησης, το οποίο μπορεί με ασφάλεια να δημοσιοποιηθεί (χωρίς να βάζει σε κίνδυνο τη μυστικότητα του κλειδιού αποκρυπτογράφησης), και το κλειδί αποκρυπτογράφησης που πρέπει να παραμείνει μυστικό, δηλαδή να είναι γνωστό μόνο σε έναν χρήστη του κρυπτοσυστήματος. Τα κλειδιά κρυπτογράφησης μπορούν να δημοσιοποιηθούν σε έναν "τηλεφωνικό κατάλογο" που περιέχει όλους τους χρήστες και τα αντίστοιχα κλειδιά κωδικοποίησής τους (στην θέση των τηλεφωνικών αριθμών). Αν ο χρήστης Α θέλει να επικοινωνήσει ιδιατέρως με τον χρήστη Β, θα πρέπει να βρει το κλειδί κρυπτογράφησης (δημόσιο κλειδί) του Β, και να κρυπτογραφήσει το μήνυμά του με αυτό το κλειδί. Τότε το κρυπτογραφημένο μήνυμα δεν μπορεί να διαβαστεί από οποιονδήποτε άλλον (ούτε από τον ίδιο τον Α), εκτός από τον χρήστη Β που κατέχει το αντίστοιχο κλειδί αποκρυπτογράφησης.

Παράδειγμα 16.5. Ένα κρυπτοσύστημα δημοσίου κλειδιού βασισμένο στο πρόβλημα ΣΑΚΙ-

ΔΙΟΥ (KNAPSACK problem).[3] Αυτό το πρόβλημα είναι γνωστό και ως κρυπτοσύστημα Merkle-Hellman, και το έχει σπάσει ο Shamir.

Το πρόβλημα ΣΑΚΙΔΙΟΥ είναι **NP**-πλήρες, οπότε θεωρείται αρκετά απρόσιτο υπολογιστικά.

Στην πραγματικότητα, γι'αυτό το κρυπτοσύστημα δεν χρησιμοποιούμε το πρόβλημα του σακιδίου, αλλά το πρόβλημα του *Αθροίσματος Υποσυνόλων (Subset Sum)*.

Το πρόβλημα του σακιδίου (για τους σκοπούς αυτού του παραδείγματος) αποτελείται από μια n-άδα $A = (a_1, \ldots, a_n)$ από διαφορετικούς θετικούς ακεραίους, που ονομάζεται διάνυσμα του σακιδίου και ένα θετικό ακέραιο k, την χωρητικότητα του σακιδίου. Το πρόβλημα είναι να βρούμε τέτοιους ακεραίους a_i των οποίων το άθροισμα να είναι ίσο με k. Προφανώς πάντα μπορεί να βρεθεί μια λύση ελέγχοντας εξαντλητικά όλα τα 2^n υποσύνολα του A, ψάχνοντας μήπως κάποιο από αυτά έχει άθροισμα το k. Για μεγάλο n αυτός ο υπολογισμός είναι απρόσιτος. Ορίζουμε μια συνάρτηση $f(x)$ ως εξής: Έστω $\vec{x}$ η δυαδική αναπαράσταση (με n bits) του ακεραίου x, $0 \leq x \leq 2^{n-1} - 1$ (προσθέτοντας μηδενικά στην αρχή, αν είναι απαραίτητο). Το $f(x)$ είναι ίσο με το άθροισμα όλων των a_i τέτοιων ώστε το i-οστό bit του x να είναι άσσος. Για παράδειγμα:

$$\begin{aligned} f(1) &= f(0\ldots001) = a_n \\ f(3) &= f(0\ldots011) = a_{n-1} + a_n \end{aligned}$$

Χρησιμοποιώντας πολλαπλασιασμό διανυσμάτων μπορούμε να συμβολίσουμε: $f(x) = A \cdot B_x$ όπου A είναι το διάνυσμα σακιδίου και B_x είναι η δυαδική αναπαράσταση του x γραμμένη ως διάνυσμα-στήλη.

Με τον παραπάνω ορισμό είναι εύκολο να υπολογίσουμε το $f(x)$ από το x, ενώ το να υπολογίσουμε το x από το $f(x)$ είναι ισοδύναμο με το να λύσουμε το πρόβλημα του σακιδίου, αφού το x αναπαριστά (στη δυαδική του μορφή) τα αντικείμενα του A που έχουν άθροισμα $f(x)$.

Η συνάρτηση $f(x)$ μπορεί να χρησιμοποιηθεί για κρυπτογράφηση με σχετικά απλό τρόπο: Το αρχικό κείμενο γράφεται με τη μορφή δυαδικής ακολουθίας αντικαθιστώντας κάθε γράμμα του αλφαβήτου με τον αντίστοιχο αριθμό (π.χ. ASCII) (γραμμένο σε δυαδική μορφή). Κάθε ακουλουθία των n bits κρυπτογραφείται υπολογίζοντας τη συνάρτηση f για το συγκεκριμένο κομμάτι (block). Η αποκρυπτογράφηση, από την άλλη πλευρά, είναι εξίσου δύσκολη με ένα NP-πλήρες πρόβλημα, όχι μόνο για τον κρυπταναλυτή, αλλά και για τον ίδιο το χρήστη. Αυτό μπορεί να αποφευχθεί σχεδιάζοντας το σύστημα έτσι ώστε ο νόμιμος χρήστης (που γνωρίζει μια μυστική καταπακτή) να χρειάζεται να λύσει ένα εύκολο στιγμιότυπο του προβλήματος του σακιδίου, ενώ ο κρυπταναλυτής να βρίσκεται απέναντι στο γενικό (δύσκολο) πρόβλημα.

Υπάρχουν κλάσεις από εύκολα προβλήματα σακιδίου. Μια τέτοια κλάση αποτελείται από τα προβλήματα σακιδίου που χρησιμοποιούν υπεραυξητικά διανύσματα σακιδίου A. Ένα διάνυ-

[3] Το πρόβλημα KNAPSACK ορίζεται ως εξής: Θεωρήστε έναν ακέραιο (την *χωρητικότητα*) $M > 0$ και ένα σύνολο S αντικειμένων s_i, που στο καθένα αντιστοιχούν δύο αριθμοί: η *τιμή* v_i, και το *βάρος* w_i. Έτσι, $S = \{s_1, \ldots, s_n\}$ όπου $s_i = (v_i, w_i)$. Το πρόβλημα είναι να βρεθεί ένα υποσύνολο $S' \subset \{1, 2 \ldots, n\}$ τέτοιο ώστε τα μέλη του να ικανοποιούν τη συνθήκη $\sum_{i \in S'} w_i \leq M$ και $\sum_{i \in S'} v_i$ να είναι όσο το δυνατόν μεγαλύτερο. Αυτό σημαίνει ότι, πρέπει να επιλέξουμε ορισμένα αντικείμενα από το S (χωρίς επαναλήψεις), τέτοια ώστε να μεγιστοποιήσουμε τη συνολική τους τιμή, ενώ τα βάρη τους να μην ξεπερνούν τη χωρητικότητα M.

σμα σακιδίου (ή μια n-άδα γενικά) $A = (a_1, \ldots, a_n)$ λέγεται *υπεραυξητική* αν κάθε αριθμός a_i υπερβαίνει το άθροισμα όλων των προηγούμενων αριθμών:

$$a_j > \sum_{i=1}^{j-1} a_i, \ for\ j = 2, \ldots, n$$

Σε αυτή την περίπτωση το πρόβλημα του σακιδίου μπορεί να λυθεί σε *γραμμικό χρόνο* αφού ένα πέρασμα του διανύσματος του σακιδίου είναι αρκετό. Είναι επίσης προφανές (από τον αλγόριθμο που λύνει το πρόβλημα) ότι το υπεραυξητικό πρόβλημα σακιδίου έχει πάντα *το πολύ μία λύση*.

Εάν χρησιμοποιούμε υπεραυξητική ακολουθία A για ένα κρυπτοσύστημα, δεν πρέπει να τη δημοσιεύσουμε, γιατί θα έκανε την κρυπτανάλυση γραμμική (άρα εύκολη). Αυτό μπορούμε να το αποφύγουμε ανακατεύοντας το A σε ένα διάνυσμα A' που θα μοιάζει με ένα τυχαίο διάνυσμα σακιδίου. Το ανακάτεμα αυτό μπορεί να γίνει με πολλαπλασιασμό με modulo:

Διαλέγουμε έναν ακέραιο (modulus) $m > \sum a_i$ και έναν πολλαπλασιαστή t έτσι ώστε ο t και ο m να μην έχουν κοινούς παράγοντες. Η εκλογή του t εξασφαλίζει την ύπαρξη του t^{-1} (αντίστροφος του t) έτσι ώστε $tt^{-1} = 1 \pmod m$. Υπολογίζουμε τα γινόμενα $a'_i = ta_i$ και ορίζουμε το διάνυσμα $A = (a'_1, \ldots, a'_n)$. Το διάνυσμα $A' = tA$ μπορεί να δημοσιευτεί ως κλειδί κρυπτογράφησης, αλλά οι όροι t, t^{-1}, m πρέπει να κρατηθούν μυστικοί (secret trapdoor).

Ο νόμιμος αποδέκτης, για να αποκρυπτογραφήσει ένα block κρυπτοκειμένου c' (block με n bits) πρέπει πρώτα να υπολογίσει το $c = t^{-1}c' \bmod m$, και μετά να λύσει το εύκολο πρόβλημα σακιδίου βασισμένο στο $A = t^{-1}A' \bmod m$. Η μοναδική λύση είναι το σωστό block αρχικού κειμένου p αφού:

$$c = t^{-1}c' = t^{-1}A'p = t^{-1}tAp = Ap \pmod m$$

που σημαίνει ότι παρόλο που η κρυπτογράφηση έγινε χρησιμοποιώντας το A', η αποκρυπτογράφηση μπορεί να βασιστεί στο A και τους μυστικούς όρους. Αυτό το κρυπτοσύστημα δημοσίου κλειδιού που βασίζεται στο πρόβλημα του σακιδίου έσπασε από τον Shamir [12] με αλγόριθμο πολυωνυμικού χρόνου. Η κρυπταναλυτική επίθεση βασίζεται στο γεγονός ότι δεν είναι απαραίτητο για τον κρυπταναλυτή να βρει τον ίδιο πολλαπλασιαστή t και modulus m με αυτα που χρησιμοποιεί ο σχεδιαστής του συστήματος. Αρκεί να βρει t' και m' τέτοια ώστε ο πολλαπλασιασμός του δημοσιευμένου διανύσματος με το $(t')^{-1} \pmod{m'}$ να είναι ένα υπεραυξητικό διάνυσμα. Έτσι, ο κρυπταναλυτής μπορεί να σπάσει το σύστημα με προεπεξεργασία, αφού το κλειδί δημοσιευτεί. □

16.5.2 Σχεδιάζοντας ένα κρυπτοσύστημα δημοσίου κλειδιού

Ένα κρυπτοσύστημα δημοσίου κλειδιού μπορούμε να το κατασκευάσουμε με τα ακόλουθα γενικά βήματα:

- Διαλέγουμε ένα δύσκολο πρόβλημα Π. Το Π θα πρέπει να είναι υπολογιστικά απρόσιτο. Το Π λέγεται υποκείμενο πρόβλημα.
- Βρίσκουμε ένα εύκολο υποπρόβλημα Π_{easy} του Π. Το Π_{easy} θα πρέπει να χρειάζεται μικρό πολυωνυμικό χρόνο.

- "Ανακατεύουμε" το Π_{easy} με τέτοιο τρόπο ώστε το προκύπτον πρόβλημα Π_{shuffle} να μοιάζει με το γενικό πρόβλημα Π.
- Δημοσιεύουμε το Π_{shuffle} και τη μέθοδο κρυπτογράφησης. Η μέθοδος ανάκτησης του Π_{easy} από το Π_{shuffle} είναι η μυστική καταπακτή. Έτσι ο νόμιμος αποδέκτης θα πρέπει να λύσει το Π_{easy} ενώ ο κρυπταναλυτής βρίσκεται ενάντια στο γενικό πρόβλημα Π.

Το κρυπτοσύστημα στο παράδειγμα 16.5 είναι μια τυπική επίδειξη των παραπάνω στοιχείων για το σχεδιασμό κρυπτοσυστημάτων δημοσίου κλειδιού: Π είναι το πρόβλημα σακιδίου (NP-πλήρες), Π_{easy} είναι το πρόβλημα σακιδίου με υπεραυξητικό διάνυσμα σακιδίου και το Π_{shuffle} προκύπτει από πολλαπλασισμό modulo όπως περιγράψαμε παραπάνω.

Η κρυπτανάλυση του κρυπτοσυστήματος δημοσίου κλειδιού (υπολογισμός του $f^{-1}(x)$ από το x χωρίς να ξέρουμε τη μυστική καταπακτή) περιλαμβάνει τη λύση του γενικού απρόσιτου προβλήματος (του υποκείμενου προβλήματος) που έχει επιλεχτεί προσεκτικά από το σχεδιαστή του συστήματος (πρόβλημα Π, σύμφωνα με την παραπάνω συζήτηση). Στο παράδειγμα 16.5, παρόλο που χρησιμοποιήθηκε ένα πρόβλημα αποδεδειγμένα απρόσιτο (πρόβλημα σακιδίου, **NP**-πλήρες), το κρυπτοσύστημα που προέκυψε, αποδείχτηκε ότι είναι μάλλον ασθενές. Από την άλλη πλευρά, το πιο μελετημένο κρυπτοσύστημα δημοσίου κλειδιού που υπάρχει (ως τώρα), το RSA, έχει αντέξει σε όλες τις κρυπταναλυτικές επιθέσεις, παρόλο που η πολυπλοκότητα του υποκείμενου προβλήματος (παραγοντοποίηση) δεν έχει κατηγοριοποιηθεί (η παραγοντοποίηση *δεν έχει αποδειχθεί ακόμη* αν είναι όντως απρόσιτο πρόβλημα, αν και πιστεύεται ευρύτατα ότι είναι).

Τα περισσότερα συστήματα δημοσίου κλειδιού βασίζονται σε αριθμοθεωρητικά υποκείμενα προβλήματα. Ο παρακάτω κατάλογος απαριθμεί μερικά θεμελιώδη αριθμοθεωρητικά προβλήματα που έχουν αντισταθεί ως τώρα σε όλες τις προσπάθειες να ταξινομηθεί η πολυπλοκότητά τους και έχουν αποδειχτεί πολύ χρήσιμα στην κρυπτογραφία δημοσίου κλειδιού. Κανένα από αυτά τα προβλήματα δεν είναι γνωστό να είναι πλήρες για κάποια κλάση πολυπλοκότητας ή να έχει κάποιο ντετερμινιστικό ή πιθανοτικό πολυωνυμικό αλγόριθμο.

FACTOR(n)	Βρές τους πρώτους παράγοντες του n
SQUAREFREENESS(n)	Αποφάσισε αν το τετράγωνο ενός πρώτου διαιρεί το n (Αποφάσισε αν το n είναι γινόμενο διακριτών πρώτων)
QUAD-RESIDUE(a, n)	Αποφάσισε αν $x^2 = a \pmod n$ ισχύει για κάποιο x
SQUAREROOT(a, n)	Βρές ένα x τέτοιο ώστε $x^2 = a \pmod n$
DISCRETE-LOG(a, b, n)	Βρές ένα x τέτοιο ώστε $a^x = b \pmod n$

16.5.3 Κρυπτανάλυση και ασφάλεια

Τυπικά, θα ήταν επιθυμητό να βρούμε ένα κάτω όριο στην ποσότητα των υπολογισμών που είναι απαραίτητοι στον κρυπταναλυτή για να σπάσει το κρυπτοσύστημα δημοσίου κλειδιού (να λύσει το υποκείμενο πρόβλημα). Δυστυχώς, τέτοια θεωρητικά κάτω όρια δεν έχουν αποδειχτεί για κανένα από τα πιο γνωστά συστήματα δημοσίου κλειδιού. Για παράδειγμα, αν το FACTOR(n)

λύνεται σε χαμηλό πολυωνυμικό χρόνο (πράγμα μάλλον απίθανο), τότε το RSA και συναφή συστήματα θα κατέρρεαν.

Ακόμη, το πρόβλημα της κρυπτανάλυσης (με δεδομένο το κρυπτοκείμενο και το κλειδί κρυπτογράφησης) για ένα σύστημα δημοσίου κλειδιού, είναι στο $NP \cap co - NP$ και άρα είναι μάλλον απίθανο ότι κάποιο πρόβλημα κρυπτανάλυσης θα είναι NP-πλήρες (γιατί θα σήμαινε ότι NP=co-NP). Από την άλλη πλευρά, για το σενάριο "κλειδί κρυπτογράφησης μόνο", το πρόβλημα κρυπτανάλυσης είναι συνήθως NP-πλήρες.

Συνήθως για να παρουσιάσουμε μια απόδειξη της ασφάλειας ενός συγκεκριμένου συστήματος δημοσίου κλειδιού, πρέπει να κατασκευάσουμε μια αναγωγή, όπου δείχνουμε πως να λύσουμε ένα δύσκολο πρόβλημα (π.χ. παραγοντοποίηση) εάν έχουμε τη δυνατότητα να σπάσουμε το κρυπτογραφικό σύστημα. Στο σχεδιασμό συστήματος δημοσίου κλειδιού, πολλές παράμετροι (όπως το μέγεθος του κλειδιού) πρέπει να καθοριστούν με βάση την υπολογιστική δύναμη που υποτίθεται ότι έχει ο επίδοξος εχθρός που προσπαθεί να σπάσει το σύστημα. Είναι πάντα συνετό να επιτυγχάνουμε η επίθεση με πολυωνυμικό χρόνο να είναι όχι μόνο πιθανοτική, αλλά και μη-ομοιόμορφη. Περισσότερο τυπική μελέτη αυτών των θεμάτων γίνεται στο κεφάλαιο **??**.

16.6 Στόχοι της Κρυπτολογίας

Καθώς οι υπολογιστές και τα δίκτυα υπολογιστών συνεχίζουν να αναπτύσσονται και να επεκτείνονται, οι εφαρμογές της κρυπτολογίας μεγαλώνουν όπως και η ανάγκη για κρυπτογραφικά συστήματα.

Η κρυπτολογία παρέχει μεθόδους ώστε να ικανοποιούνται οι βασικές απαιτήσεις ασφαλούς επικοινωνίας. Μερικές από αυτές, και κάποιες πιο εξειδικευμένες, αναφέρονται παρακάτω (βλ. και [**?**]):

- *Μυστικότητα (Privacy)*. Ο πιθανός "κατάσκοπος" να μην μαθαίνει τίποτα χρήσιμο για το μήνυμα που στάλθηκε.
- *Πιστοποίηση (Authentication)*. Ο αποδέκτης του μηνύματος να μπορεί να πειστεί ότι το μήνυμα εστάλη πράγματι από τον υποτιθέμενο αποστολέα.
- Εμπιστευτικότητα (confidentiality): κανείς μη εξουσιοδοτημένος χρήστης δεν πρέπει να έχει πρόσβαση στο μεταδιδόμενο μήνυμα.
- Έλεγχος ακεραιότητας των δεδομένων (data integrity): αλλοίωση των δεδομένων κατά τη μετάδοση πρέπει να γίνεται αντιληπτή στον παραλήπτη.
- *Υπογραφές (Signatures)*. Ο αποδέκτης ενός μηνύματος να μπορεί να πείσει κάποιον τρίτο ότι το μήνυμα πράγματι εστάλη από τον υποτιθέμενο αποστολέα.
- *Μη Αποκήρυξη (Non-Repudiation)*: κανείς δεν μπορεί να αποποιηθεί την υπογραφή του.
- *Ελαχιστότητα (Minimality)*. Τίποτα δεν κοινοποιείται στους άλλους, εκτός από αυτό που ρητά επιθυμούμε να κοινοποιήσουμε.

- *Ταυτόχρονη Αμοιβαία Ανταλλαγή (Simultaneous Exchange)*. Κάτι πολύτιμο (π.χ. υπογραφή σε συμβόλαιο), δεν πρέπει να αποστέλλεται εωσότου κάτι άλλο πολύτιμο (π.χ. η υπογραφή του άλλου) να παραληφθεί.

- *Συντονισμός (Coordination)*. Σε επικοινωνία μεταξύ πολλών πλευρών, οι πλευρές μπορούν να συντονίσουν τις ενέργειές τους για την επίτευξη κοινών στόχων ακόμη και με την παρουσία αντιπάλων (κατασκόπων).

- *Κατώφλι Συνεργασίας (Collaboration Threshold)*. Σε ένα σενάριο με πολλές πλευρές, οι επιθυμητές ιδιότητες ισχύουν μόνο για όσο ο αριθμός των αντιπάλων δεν υπερβαίνει το δεδομένο κατώφλι (όριο).

- *Μερική Αποκάλυψη Απορρήτων (Partial Disclosure of Secrets)*. Δύο η περισσότερες πλευρές που κατέχουν τα απόρρητα $x1, x2, \ldots$, επιθυμούν να διανείμουν την τιμή της $f(x1, x2, \ldots)$ χωρίς να αποκαλύψουν τα $x1, x2, \ldots$ σε κανέναν άλλο.

- *Μη Συνειδητή Μεταφορά (Oblivious Transfer)*. Η πλευρά Α που κατέχει ένα απόρρητο θέλει να το μεταφέρει σε μια άλλη πλευρά Β, έτσι ώστε η Α να μη γνωρίζει αν η Β παρέλαβε το μυστικό (αλλά η Β το γνωρίζει). Ή, η Α κατέχει πολλά μυστικά και θέλει να μεταφέρει μόνο ένα στη Β έτσι ώστε μόνο η Β να γνωρίζει ποιο μυστικό μεταφέρθηκε.

- *Αποδείξεις και Πρωτόκολλα Μηδενικής Γνώσης (Zero-Knowledge Proofs and Protocols)*. Κατά την εκτέλεση ενός πρωτοκόλλου, κανείς (ούτε οι νόμιμοι συμμετέχοντες) δεν μπορεί να μάθει τίποτε άλλο, εκτός από αυτό που προβλέπεται από το πρωτόκολλο.

- *Ανώνυμες Δοσοληψίες (Anonymous Transactions)*, ψηφιακά ψευδώνυμα (anonymous credentials). Έγκυρα ψηφιακά πιστοποιητικά που δεν μπορούν να συνδεθούν με τον πραγματικό κάτοχο.

- Τράπεζες, ψηφοφορίες, κρυπτονομίσματα (cryptocurrencies, π.χ. bitcoin) και άλλες μη θεωρητικές εφαρμογές….

Από την άλλη πλευρά, η *κρυπτανάλυση (cryptanalysis)* Κρυπτανάλυση ορίζεται ως η μελέτη των μαθηματικών τεχνικών που αποσκοπούν στην παραβίαση, σε ένα κρυπτογραφικό σύστημα, των παραπάνω χαρακτηριστικών. Το κρυπτόγραμμα, εφόσον μεταδίδεται μέσα από δημόσιο τηλεπικοινωνιακό κανάλι, είναι διαθέσιμο στον οποιονδήποτε, ακόμα και στον επίδοξο υποκλοπέα. Η εμπιστευτικότητα σε ένα κρυπτογραφικό σύστημα παραβιάζεται αν κάποιος υποκλοπέας καταφέρει τελικά, χωρίς τη γνώση του κλειδιού, να διαβάσει το αρχικό μήνυμα (ή, ισοδύναμα, να ανακαλύψει το κλειδί αποκρυπτογράφησης). Έχουν αναπτυχθεί πολλές κρυπταναλυτικές τεχνικές για όλα τα είδη κρυπτογραφικών αλγορίθμων. Η εμφάνιση κάθε κρυπταναλυτικής τεχνικής έχει εν τέλει ως αποτέλεσμα το να καθορίζονται νέες σχεδιαστικές αρχές που πρέπει να λαμβάνονται υπ' όψιν κατά την κατασκευή κρυπτογραφικών αλγορίθμων. Κατά συνέπεια, η κρυπτογραφία και η κρυπτανάλυση συμβαδίζουν ως προς την εξέλιξή τους. Ο όρος *κρυπτολογία (cryptology)* Κρυπτολογία έχει παγιωθεί, προκειμένου να συμπεριλαμβάνει ταυτόχρονα τόσο την κρυπτογραφία όσο και την κρυπτανάλυση.

16.7 Μοντέλα ασφάλειας

Για να συζητήσουμε για την ασφάλεια, χρειάζεται να ορίσουμε κάποιο *μοντέλο ασφάλειας*, που περιγράφει συνήθως τις δυνατότητες του αντιπάλου. Κατ'αρχήν, δεχόμαστε την παρακάτω βασική υπόθεση.

Θεμελιώδης αρχή (Kerckhoffs): όλοι οι αλγόριθμοι είναι γνωστοί, *μόνο το κλειδί είναι άγνωστο* (μην υποτιμάς τον αντίπαλο!).

Με βάση το τι διαθέτει (ή μπορεί να βρει) ο αντίπαλος ορίζονται 4 βασικοί τύποι κρυπταναλυτικών επιθέσεων:

1. Κρυπτοκείμενο μόνο (**ciphertext only – CO**). Ο κρυπταναλυτής διαθέτει μόνο το κρυπτοκείμενο.
2. Γνωστό αρχικό κείμενο (**known plaintext attack – KPA**). Ο κρυπταναλυτής διαθέτει κάποια ζεύγη αρχικού κειμένου–κρυπτοκειμένου.
3. Επιλεγμένο αρχικό κείμενο (**chosen plaintext attack – CPA**). Ο κρυπταναλυτής διαθέτει κάποια ζεύγη αρχικού κειμένου–κρυπτοκειμένου, με αρχικά κείμενα της επιλογής του.
4. Επιλεγμένο κρυπτοκείμενο (**chosen ciphertext attack – CCA**). Ο κρυπταναλυτής διαθέτει κάποια ζεύγη αρχικού κειμένου–κρυπτοκειμένου για ορισμένα κρυπτοκείμενα της επιλογής του (ισοδύναμα, έχει προσωρινή δυνατότητα αποκρυπτογράφησης).

Η σύγχρονη τάση είναι να ασχολούμαστε με συστήματα που μπορούν να αντέξουν στις πιο ισχυρές επιθέσεις CPA και CCA°η τελευταία έχει ιδιαίτερο νόημα στην κρυπτογραφία δημοσίου κλειδιού, όπου ο αντίπαλος εξ ορισμού διαθέτει να παράγει ζεύγη αρχικού κειμένου – κρυπτοκειμένου κατά βούληση.

Μια πιο πρόσφατη θεώρηση, προτείνει την περαιτέρω ισχυροποίηση των δύο ισχυρότερων μοντέλων, CPA και CCA, μέσω ενός κατάλληλα διατυπωμένου παιγνίου:

The indistiguishability game (Το παίγνιο της μη-διακρισιμότητας)

- Δίνεται ένα κρυπτοκείμενο c. Ακόμη και αν ο αντίπαλος γνωρίζει ότι το αρχικό κείμενο είναι είτε το m_0 είτε το m_1, δεν θα πρέπει να είναι σε θέση να ξεχωρίσει ποιο από τα δύο είναι το σωστό με πιθανότητα σημαντικά μεγαλύτερη από $\frac{1}{2}$.
- Μπορεί να διατυπωθεί σαν παίγνιο μεταξύ ενός αντιπάλου και ενός κρυπτοσυστήματος.
- Μπορεί να εφαρμοστεί σε όλες τις επιθέσεις. Περισσότερο γνωστό για IND-CPA και IND-CCA (και IND-CCA2) στα πλαίσια της κρυπτογραφίας δημοσίου κλειδιού (όπου εξ ορισμού ο αντίπαλος έχει δυνατότητα CPA τουλάχιστον).

16.8 Θεωρία αριθμών και Κρυπτογραφία

Τα κρυπτοσυστήματα δημοσίου κλειδιού (καθώς και τα κλασικά κρυπτοσυστήματα) χρησιμοποιούν εκτενώς πολλά θέματα της Θεωρίας Αριθμών. Η τυποποίηση των περισσοτέρων κρυπτογραφικών συστημάτων χρησιμοποιεί πολλές αριθμοθεωρητικές έννοιες καθώς επίσης και στοιχεία Αφηρημένης Άλγεβρας (Θεωρία Ομάδων - Πεπερασμένα Σώματα).

Εκτός από τις στοιχειώδεις έννοιες και συμβολισμούς, η κρυπτογραφία χρησιμοποιεί εκτενώς τη θεωρία αριθμών που αφορά ισοτιμίες, πράξεις σε πεπερασμένα σώματα και τετραγωνικά υπόλοιπα.

Ειδικότερα, η Θεωρία Αριθμών που χρειάζεται για να προσεγγίσουμε τα πιο βασικά κρυπτογραφικά συστήματα και ιδέες, περιλαμβάνει τουλάχιστον τα εξής:

- Θεμελιώδεις ορισμούς, συμβολισμούς, διαιρετότητα, τον ευκλείδιο αλγόριθμο, το θεμελιώδες θεώρημα της αριθμητικής, το θεώρημα των πρώτων αριθμών.
- Θεωρία ομάδων, δακτυλίων, σωμάτων και στοιχειώδεις αλγεβρικές έννοιες και ισοτιμίες, το Κινέζικο Θεώρημα Υπολοίπων, το Μικρό Θεώρημα του Fermat, η συνάρτηση ϕ του Euler και οι ιδιότητές της.
- Γραμμικές ισοτιμίες, πρώτοι moduli, δυναμοϋπόλοιπα, παραγοντοποίηση.
- Τετραγωνικά υπόλοιπα, σύμβολο Legendre, τετραγωνική αμοιβαιότητα, σύμβολο Jacobi.

Πολλοί αλγόριθμοι για αριθμοθεωρητικά προβλήματα, έλεγχοι για το αν ένας αριθμός είναι πρώτος, γεννήτριες τυχαίων αριθμών, έλεγχοι ασφάλειας χρησιμοποιούνται επίσης στην κρυπτογραφία.

16.9 Primality – Factoring

Ένα πολύ σημαντικό στοιχείο για την κρυπτογράφηση, αποκρυπτογράφηση, αλλά κυρίως για την κρυπτανάλυση ενός κρυπτογραφικού συστήματος είναι ο έλεγχος ενός αριθμού για το αν είναι πρώτος (primality test) αλλά και η ανάλυση σε πρώτους παράγοντες (factoring).

Η προσπάθεια να απαντηθεί το αν ένας αριθμός είναι πρώτος είναι ένα ιδιαίτερα παλιό πρόβλημα και έχει απασχολήσει πολύ τη μαθηματική κοινότητα. Ένα από τα παλιότερα primality tests είναι το *Κόσκινο του Ερατοσθένη*. Η πολυπλοκότητα του είναι πολυωνυμική ώς προς το μέγεθος της εισόδου k, αλλά εκθετική ως προς το μήκος της αναπαράστασης του k.

Μετά από τα πρώτα, παλιά αποτελέσματα που απαντούσαν στο ερώτημα με εξαντλητικές μεθόδους, είχε μείνει για πολλά χρόνια ανοιχτό το ερώτημα αν το πρόβλημα μπορεί να λυθεί σε χρόνο πολυωνυμικό ως προς το μέγεθος της εισόδου.

Σημαντικές εξελίξεις πάνω στο πρόβλημα έγιναν την δεκαετία του ’70. Το 1976 ο Miller επινόησε ένα ντετερμινιστικό αλγόριθμο που μπορούσε να δώσει απάντηση στο πρόβλημα σε πολυωνυμικό χρόνο, αλλά ο αλγόριθμος βασιζόταν στην εκτεταμένη υπόθεση του Riemann. Δηλαδή, ο Miller έδειξε οτι το πρόβλημα βρίσκεται στην κλάση **P** αν η υπόθεση του Riemann

είναι σωστή. Το τελευταίο είναι ένα από τα πλέον γνωστά ανοιχτά προβλήματα που μένουν άλυτα εδώ και 100 περίπου χρόνια αν και οι περισσότεροι θεωρούν ότι ισχύει. Ένα χρόνο μετά τον Miller, οι Solovay και Strassen δημοσίευσαν ένα νέο πιθανοτικό αλγόριθμο που έδινε απάντηση στο πρόβλημα. Λίγο αργότερα, ο Rabin τροποποίησε τον αλγόριθμο του Miller σε έναν επίσης πιθανοτικό πολυωνυμικό αλγόριθμο. Το 1983 οι Adleman, Pomerance και Rumely παρουσίασαν για πρώτη φορά μια νέα μέθοδο που αποδεχόταν το πρόβλημα των πρώτων σε χρόνο $(\log n)^{O(\log\log\log n)}$. Αν και πρακτικά σχεδόν πολυωνυμικός χρόνος, η προσπάθειά τους δεν επέτρεπε στους θεωρητικούς να θέσουν το πρόβλημα στο **P**. Το 1986 οι Goldwasser και Killian προτείνουν ένα νέο αλγόριθμο με αναμενόμενο πολυωνυμικό χρόνο απόφασης που βασιζόταν σε ελλειπτικές καμπύλες. Οι Adleman και Huang το 1992, τροποποίησαν τον αλγόριθμο των Goldwasser και Killian, δείχνοντας ότι το πρόβλημα είναι στο **ZPP** (Zero error Probabilistic Polynomial Time).

Οριστικό τέλος δόθηκε με την εργασία των Manindra Agrawal, Neeraj Kayal και Nitin Saxena που εκδόθηκε τις πρώτες μέρες του Αυγούστου του 2002 θέτοντας το πρόβλημα στο **P** (γνωστός πλέον και ως αλγόριθμος AKS). Παρά την αρχική πολύπλοκη μορφή της απόδειξης της ορθότητας του αλγορίθμου τους, δεν πέρασε πολύ καιρός για να πάρει μια πιο απλή και αποτελεσματική μορφή μετά από παρατηρήσεις του Lenstra.

Αντίθετα με το πρόβλημα Primality, για το Factoring πιστεύεται ότι δεν υπάρχει πολυωνυμικός αλγόριθμος (ντετερμινιστικός ή πιθανοτικός). Ο καλύτερος γνωστός αλγόριθμος έχει πολυπλοκότητα τάξης $2^{\tilde{O}((\log n)^{\frac{1}{3}})}$ που είναι υπερ-πολυωνυμική, αφού το πλήθος των ψηφίων του αριθμού βρίσκεται στον εκθέτη, αν και υψωμένο σε αριθμό μικρότερο του 1 (αυτό είναι ένδειξη ότι το πρόβλημα δεν είναι τόσο δύσκολο όσο τα **NP**-πλήρη). Η δυσκολία του Factoring είναι βασικό συστατικό πολλών κρυπτοσυστημάτων δημοσίου κλειδιού, με κυριότερο το RSA. Επομένως, τυχόν εύρεση αποδοτικού αλγορίθμου θα οδηγούσε σε κατάρρευση τα συστήματα αυτά. Αξίζει τέλος να σημειωθεί ότι, με βάση και όσα είπαμε παραπάνω, δεν μπορεί να αποκλειστεί το ενδεχόμενο το Factoring να επιλύεται πολυωνυμικά, ακόμη και αν $\mathbf{P} \neq \mathbf{NP}$.

16.10 Η κρυπτολογία στον σύγχρονο κόσμο

Είναι κοινός πλέον τόπος ότι οι κρυπτογραφικές εφαρμογές, πρωτόκολλα και τεχνικές έχουν κομβικό ρόλο στη σύγχρονη τεχνολογία, ειδικά στους τομείς της ασφαλούς επικοινωνίας, της ασφαλούς πρόσβασης, των ηλεκτρονικών ψηφοφοριών, της ανάκτησης και διαχείρισης ευαίσθητων δεδομένων, και των ηλεκτρονικών συναλλαγών, με πρόσφατη σημαντικότατη εξέλιξη την ανάπτυξη του κρυπτονομίσματος Bitcoin, και αρκετών ήδη διαδόχων του, με κυρίαρχο χαρακτηριστικό την απουσία κεντρικού ελέγχου.

Οι παραπάνω εφαρμογές, και πολλές άλλες που δεν αναφέρθηκαν, μπόρεσαν να πραγματοποιηθούν χάρη στην αλματώδη ανάπτυξη επαναστατικών ιδεών και αλγορίθμων, όπως η τέλεια μυστικότητα, η κρυπτογραφία δημοσίου κλειδιού, η ασφαλής ανταλλαγή κλειδιού από απόσταση, οι ψηφιακές υπογραφές, τα διαλογικά συστήματα αποδείξεων και οι αποδείξεις μηδενικής γνώσης, οι γεννήτριες ψευδοτυχαιότητας, η σύνθεση πρωτοκόλλων, οι συναρτήσεις κατακερματισμού χωρίς συγκρούσεις, η υπολογιστική πολυπλοκότητα, και πολλά άλλα.

Κοινό χαρακτηριστικό των παραπάνω μεθόδων είναι ότι η ασφάλειά τους εδράζεται, όλο και περισσότερο, σε αυστηρές μαθηματικές αποδείξεις. Για παράδειγμα, είμαστε πλέον σε θέση να διενεργούμε ηλεκτρονικές ψηφοφορίες που παρέχουν αποδείξεις ορθότητας για διάφορες φάσεις της λειτουργίας τους. Ή, να διενεργούμε συναλλαγές χωρίς κεντρική αρχή, μέσω του Bitcoin ή άλλων κρυπτονομισμάτων, με απόδειξη εγκυρότητας για κάθε συναλλαγή, που επικυρώνεται συλλογικά! Τα κρυπτονομίσματα είναι μια επανάσταση σε εξέλιξη, ανοίγοντας δρόμους για αποκεντρωμένη και αποδεδειγμένα ασφαλή ψηφιακή υλοποίηση λειτουργιών που μέχρι σήμερα απαιτούσαν την ύπαρξη κάποιας αρχής, όπως για παράδειγμα τη σύναψη συμβολαίων.

Τα μαθηματικά γίνονται για άλλη μια φορά επίκαιρα, βοηθώντας στην εμπέδωση εμπιστοσύνης σε κρίσιμες λειτουργίες, και μέσω αυτής στο άνοιγμα της κρυπτογραφίας στο πλατύ κοινό. Οι περισσότεροι αλγόριθμοι είναι πλέον τελείως ανοιχτοί, και η ασφάλειά τους βασίζεται αποκλειστικά σε αλγορίθμους που μας επιτρέπουν να εκτελούμε αποδοτικά πράξεις με αριθμούς χιλιάδων ψηφίων, ώστε η υπολογιστική δυσκολία (πολυπλοκότητα) των αντίστροφων πράξεων να είναι τεράστια. Η κρυπτογραφία έχει φύγει οριστικά από τα στεγανά των μυστικών υπηρεσιών και τη στρατιωτική χρήση και είναι έτοιμη να προσφέρει ακόμη περισσότερο τις υπηρεσίες της στο σύνολο της ανθρωπότητας πλέον, προάγοντας τη δημοκρατία, τον σεβασμό της ιδιωτικής ζωής, και τελικά την ενεργό και ισότιμη συμμετοχή όλων στο οικονομικό, πολιτικό, και κοινωνικό γίγνεσθαι.

16.11 Διαδραστικό Υλικό – Σύνδεσμοι

- Διαδραστικές Παρουσιάσεις - Video
  - Το πανεπιστήμιο του Rhode Island έχει συγκεντρώσει παρουσιάσεις κλασικών κρυπτοσυστημάτων στους παρακάτω συνδέσμους :
    * Κρυπτοσυστήματα Ολίσθησης
    * Κρυπτοσυστήματα Affine
    * Κρυπτοσυστήματα Αντικατάστασης
    * Vigenére
  - The BLACK Chamber, Διαδραστικές παρουσιάσεις κλασικών συστημάτων από τον Simon Singh, συγγραφέα ενός από τα πιο διάσημα βιβλία κρυπτογραφίας για το ευρύ κοινό
  - Προσομοιωτής Μηχανής Enigma
  - Αποσυναρμολόγηση Μηχανής Enigma
  - Ανακατασκευή μηχανής Bombe του Turing
  - Επίδειξη τέλειας μυστικότητας Shannon
  - Διαλέξεις για αποδείξεις μέσω κρυπτογραφικών αναγωγών
- Διαδραστικές Υλοποιήσεις
  - Sharky's Vigenére Cipher

  - Vigenére Cipher Codebreaker

- Κώδικας
  - Βιβλιοθήκη κλασικών κρυπτοσυστημάτων στο Sage
  - Μηχανή Enigma σε Javascript
  - Κρυπτογράφηση και κρυπτανάλυση κλασικών κρυπτοσυστημάτων σε Python

Βιβλιογραφία

[1] M. Bellare and S. Goldwasser. *Lecture notes in Cryptography*. 1995.

[2] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.

[3] J. Daemen and V. Rijmen. *The Design of Rijndael:AES-The Advanced Encryption Standard*. Springer, 2002.

[4] S. Haber and W.S. Stornetta. How to timestamp a digital document. *Journal of Cryptology*, 3:pp 99–111, 1991.

[5] D. Kahn. *The Codebreakers. The Story of Secret Writing.* Macmillan, 1967.

[6] Neal Koblitz. *A Course in Number Theory and Cryptography*. Springer Verlag, 1994.

[7] Evangelos Kranakis. *Primality and Cryptography*. John Wiley & Sons, 1987.

[8] Ralph C. Merkle. Secure communications over insecure channels. *Communications of the ACM*, 21(4):294–299, April 1978.

[9] A. J. Menezes, P.C van Oorschot, and S. A. Vanstone. *Handbook of applied cryptography*. CRC Press, 1996.

[10] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[11] C. E. Shannon. A mathematical theory of communication. *Bell Systems Technical Journal*, 27:379–423, 623–656, 1948.

[12] A Shamir. A polynomial-time algorithm for breaking the basic merkle-hellman cryptosystem. *Transactions on Information Theory*, 30:pp 699–704, 1984.

[13] Douglas R. Stinson. *Cryptography. Theory and Practice.* Discrete Mathematics and its Applications. CRC Press, 1995.

[14] C. E. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[15] A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.

[16] Bluetooth SIG, Specification of the Bluetooth system, version 1.1, February 22, 2001, http://www.bluetooth.com.

[17] M. Bellare and S. Goldwasser. *Lecture notes in Cryptography*. 1995.

[18] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", The Cryptography Mailing list at metzdowd.com, 2008.