6 ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

6.1. Εισαγωγή

Οι σύγχρονες κρυπτογραφικές λύσεις συμπεριλαμβάνουν κρυπτογραφία δημόσιου κλειδιού ή αλλιώς, ασύμμετρη κρυπτογραφία. Η ασύμμετρη κρυπτογραφία βασίζεται αποκλειστικά σε μαθηματικές υποθέσεις για τον λόγο ότι υπάρχει μαθηματική εξάρτηση μεταξύ του δημόσιου και του ιδιωτικού κλειδιού. Η ασφάλεια επομένως εξαρτάται από την πληροφορία που διαρρέει από το δημόσιο κλειδί, όσον αφορά το ιδιωτικό κλειδί.

Όταν αναφερόμαστε σε κρυπτοσύστημα δημόσιου κλειδιού, χρησιμοποιούμε τον όρο «ιδιωτικό κλειδί», για να αναφερθούμε στη μυστική ποσότητα που δεν είναι γνωστή στο ευρύτερο κοινό και ειδικότερα στον αντίπαλο. Αυτός ο όρος χρησιμοποιείται για λόγους διάκρισης από τα συμμετρικά κρυπτοσυστήματα, όπου η μυστική ποσότητα αναφέρεται ως «μυστικό κλειδί».

Σε αντίθεση με τη συμμετρική κρυπτογραφία, σε ένα ασύμμετρο κρυπτοσύστημα ο αλγόριθμος κρυπτογράφησης είναι ίδιος με τον αλγόριθμο αποκρυπτογράφησης, με τη μόνη διαφορά ότι κατά την αποκρυπτογράφηση χρησιμοποιείται το αντίστοιχο κλειδί. Έτσι, σε ένα ασύμμετρο κρυπτοσύστημα όπου το ζευγάρι του δημόσιου και ιδιωτικού κλειδιού είναι το (k_e, k_d), αν η κρυπτογράφηση ορίζεται από την πράξη e_{k_e}, τότε για την αποκρυπτογράφηση θα ισχύει:

$$d_{k_d}(x) = e_{k_d}(x) .$$

Λόγω της συμμετρίας των πράξεων, αν η κρυπτογράφηση είναι η e_{k_d}, τότε η αποκρυπτογράφηση θα ορίζεται από την e_{k_e}.

6.2. Μονόδρομες συναρτήσεις με μυστική πόρτα

Στο Κεφάλαιο 4 αναφερθήκαμε στις μονόδρομες συναρτήσεις. Μια συνάρτηση f είναι μονόδρομη, όταν δοθέντος x μπορεί να υπολογιστεί η $f(x)$ με ευκολία, ενώ δοθέντος y, είναι υπολογιστικά αδύνατο να βρεθεί το $x = f^{-1}(y)$. Η έννοια του *εύκολου* υπολογισμού, αναφέρεται στις σχέσεις οι οποίες μπορούν να υπολογιστούν

σε χρόνο που καθορίζεται από πολυωνυμική συνάρτηση χρόνου σε σχέση με την είσοδο. Η περιγραφή της έννοιας του υπολογιστικά αδύνατου και ειδικότερα ο καθορισμός των ορίων μεταξύ του υπολογιστικά αδύνατου και του υπολογιστικά δυνατού είναι ένα από τα άλυτα προβλήματα της θεωρίας πολυπλοκότητας και δεν θα επεκταθούμε περισσότερο στο σημείο αυτό.

Από τις μονόδρομες συναρτήσεις, αυτές που έχουν χρησιμότητα στην ασύμμετρη κρυπτογραφία είναι οι μονόδρομες συναρτήσεις με μυστική πόρτα.

ΟΡΙΣΜΟΣ 6.1 – Μια μονόδρομη συνάρτηση με μυστική πόρτα είναι η οικογένεια αντιστρέψιμων συναρτήσεων f_k με τα παρακάτω χαρακτηριστικά:

- δοθέντων k, x, ο υπολογισμός της $y = f_k(x)$ είναι εύκολος,
- δοθέντων k, y, ο υπολογισμός της $x = f_k^{-1}(y)$ είναι εύκολος,
- δοθέντος y, ο υπολογισμός της $y = f_k^{-1}(x)$ είναι αδύνατος.

Η ποσότητα k ονομάζεται ***μυστική πόρτα*** και είναι η ποσότητα εκείνη που απαιτείται για να είναι δυνατή η αντιστροφή της f_k.

Με βάση την παραπάνω θεωρία, οι Diffie και Hellman εισήγαγαν την έννοια του ασύμμετρου κρυπτοσυστήματος. Σύμφωνα με τους Diffie και Hellman (1976), ένα ασύμμετρο κρυπτοσύστημα θα πρέπει να πληροί τις ακόλουθες απαιτήσεις:

- Είναι υπολογιστικά εύκολο για τον Βύρωνα να δημιουργήσει ένα ζεύγος κλειδιών, ke_b (δημόσιο κλειδί) και kd_b (ιδιωτικό κλειδί).
- Είναι υπολογιστικά εύκολο για την Αλίκη, η οποία γνωρίζει το δημόσιο κλειδί του Βύρωνα, να κρυπτογραφήσει ένα μήνυμα p με την κρυπτογραφική πράξη:

$$c = e_{ke_b}(p)$$

- Είναι υπολογιστικά εύκολο για τον Βύρωνα, ο οποίος γνωρίζει το ιδιωτικό του κλειδί, να αποκρυπτογραφήσει το c με την κρυπτογραφική πράξη:

$$p = d_{kd_b}(c)$$

- Είναι υπολογιστικά αδύνατο για τον αντίπαλο ο οποίος γνωρίζει το δημόσιο κλειδί του Βύρωνα ke_b, να καθορίσει το ιδιωτικό κλειδί του Βύρωνα kd_b.
- Είναι υπολογιστικά αδύνατο για τον αντίπαλο, ο οποίος γνωρίζει το δημόσιο κλειδί του Βύρωνα ke_b και το κρυπτοκείμενο c, να ανακαλύψει το απλό κείμενο p.

6.3. Ο αντίπαλος

Τα δύο τελευταία κριτήρια των Diffie και Hellman απευθύνονται στον αντίπαλο και περιγράφουν τους δύο στόχους του. Ο πρωταρχικός στόχος του αντιπάλου είναι να μπορέσει να αντιστοιχήσει τα κρυπτοκείμενα που λαμβάνει ο Βύρων στα

απλά κείμενα. Αν ο αντίπαλος ανακαλύψει συστηματικό τρόπο με τον οποίο μπορεί να αντιστοιχεί κρυπτοκείμενα σε απλά κείμενα, τότε θεωρούμε ότι το κρυπτοσύστημα έχει σπάσει μερικώς.

Ο δεύτερος στόχος του αντιπάλου είναι η ανακάλυψη του ιδιωτικού κλειδιού του Βύρωνα. Σε περίπτωση επιτυχίας θα μπορεί να αποκρυπτογραφήσει όλα τα μηνύματα που προορίζονται για τον Βύρωνα και είναι κρυπτογραφημένα με το δημόσιό του κλειδί. Αν ο αντίπαλος επιτύχει τον στόχο του, θεωρούμε ότι το κρυπτοσύστημα έχει σπάσει πλήρως.

Η διαφοροποίηση των επιθέσεων ως προς τους παραπάνω στόχους είναι αναγκαία στην ασύμμετρη κρυπτογραφία και σε αυτό οφείλεται η γνώση του δημόσιου κλειδιού. Μια πιθανή επίθεση του αντιπάλου όσον αφορά τον πρώτο στόχο, είναι η συστηματική κρυπτογράφηση απλών κειμένων με το δημόσιο κλειδί, έως ότου προκύψει κρυπτοκείμενο ίδιο με το ζητούμενο. Ο αντίπαλος χωρίς να γνωρίζει το ιδιωτικό κλειδί, μπορεί να ανακαλύψει το απλό κείμενο. Αυτή η επίθεση ονομάζεται ***επίθεση πιθανού μηνύματος*** (probable message attack).

6.3.1. Μοντέλα επίθεσης

Η ευκαιρία επίθεσης γνωστού απλού κειμένου υπάρχει έμφυτη στα ασύμμετρα κρυπτοσυστήματα. Ο αντίπαλος γνωρίζοντας το δημόσιο κλειδί, έχει τόσο τη δυνατότητα όσο και την ευκαιρία να δημιουργεί σημαντικές ποσότητες ζευγαριών απλού κειμένου και κρυπτοκειμένου, κάτω από το δημόσιο κλειδί.

Σε ορισμένες εφαρμογές ο αντίπαλος έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης, χωρίς να έχει πρόσβαση στο ίδιο το ιδιωτικό κλειδί. Σε αυτήν την περίπτωση ο αντίπαλος έχει τη δυνατότητα επίθεσης επιλεγμένου κρυπτοκειμένου, ή επίθεσης προσαρμοσμένου κρυπτοκειμένου. Κατά την επίθεση επιλεγμένου κρυπτοκειμένου ο αντίπαλος παρέχει στο κρυπτοσύστημα κρυπτοκείμενα και ζητάει την αποκρυπτογράφησή τους. Είναι προφανές ότι ο πρώτος στόχος του αντιπάλου, η αποκρυπτογράφηση των κρυπτοκειμένων, έχει εκπληρωθεί σε αυτό το μοντέλο, οπότε ο στόχος του αντιπάλου αυτόματα μετατρέπεται στην απόπειρα ανάκτησης του ιδιωτικού κλειδιού.

Με βάση την ευκαιρία πρόσβασης στον αλγόριθμο αποκρυπτογράφησης, ανάλογα με το κρυπτοσύστημα, ο αντίπαλος μπορεί να τροποποιήσει την παραπάνω επίθεση και να εκτελέσει επίθεση προσαρμοσμένου κρυπτοκειμένου. Κατά την επίθεση αυτή, ο αντίπαλος επιλέγει την επόμενη αποκρυπτογράφηση με βάση το αποτέλεσμα της προηγούμενης αποκρυπτογράφησης. Λόγω του χαρακτηριστικού της ασύμμετρης κρυπτογραφίας όπου ο αλγόριθμος κρυπτογράφησης και αποκρυπτογράφησης διαφέρουν μόνον στο κλειδί, σε ορισμένα ασύμμετρα κρυπτοσυστήματα η διαδοχική αποκρυπτογράφηση ή κρυπτογράφηση ενός μηνύματος οδηγεί μετά από πολλές επαναλήψεις στο αρχικό μήνυμα. Ο αντίπαλος μπορεί να χρησιμοποιήσει την πληροφορία αυτή για να ανακτήσει το ιδιωτικό κλειδί.

Εμπιστευτικότητα και ακεραιότητα

Η γνώση του δημόσιου κλειδιού του παραλήπτη Βύρωνα είναι καθοριστικός παράγοντας για την εμπιστευτικότητα των μηνυμάτων που αποστέλλονται σε αυτόν. Η επίθεση του ενδιάμεσου ατόμου που περιγράφεται στο Κεφάλαιο 1 δείχνει την αδυναμία της ασύμμετρης κρυπτογραφίας να προσφέρει εμπιστευτικότητα στα επικοινωνούντα μέλη. Έτσι προκειμένου να προστατευθεί η εμπιστευτικότητα, η ασύμμετρη κρυπτογραφία συνοδεύεται στην πράξη από κρυπτογραφικά πρωτόκολλα ασφαλείας τα οποία θα εξετάσουμε στο Κεφάλαιο 9. Όσον αφορά λοιπόν την εμπιστευτικότητα, αυτή παρέχεται με μηχανισμούς πιστοποίησης των δημοσίων κλειδιών, όπως θα παρουσιάσουμε στο Κεφάλαιο 8.

Οι μηχανισμοί επίδρασης του ασύμμετρου κρυπταλγόριθμου στο απλό κείμενο είναι ανάλογοι με αυτούς των συμμετρικών κρυπταλγόριθμων τμήματος. Έτσι και στην περίπτωση της ασύμμετρης κρυπτογραφίας, το απλό κείμενο χωρίζεται σε τμήματα συγκεκριμένου μήκους και το κάθε τμήμα κρυπτογραφείται ξεχωριστά. Αυτό δίνει την ευκαιρία στον αντίπαλο να αναδιατάξει τα τμήματα του κρυπτοκειμένου, ώστε η αποκρυπτογράφηση να δώσει μήνυμα άλλο από το αρχικό απλό κείμενο. Συνεπώς, στην περίπτωση της ασύμμετρης κρυπτογραφίας είναι αναγκαίο να συνδυαστεί ο κρυπτογραφική πράξη με μονόδρομες MAC, όπως συμβαίνει και στη συμμετρική κρυπτογραφία.

6.4. Κρυπτοσυστήματα knapsack

Τα κρυπτοσυστήματα knapsack βασίζονται στο γνωστό πρόβλημα του «αθροίσματος των γραμματοσήμων» που θεωρείται δύσκολο. Έστω ότι έχουμε στη διάθεσή μας έναν αριθμό γραμματοσήμων, όπου το κάθε γραμματόσημο έχει συγκεκριμένη αξία από το σύνολο τιμών $\{b_1,b_2,\ldots, b_n\}$. Το πρόβλημα είναι όταν μας δίνεται ένα γράμμα αξίας S, να βρούμε εκείνον το συνδυασμό των γραμματοσήμων των οποίων το άθροισμα τιμών είναι ίσο με S.

Σίγουρα από την εμπειρία μας γνωρίζουμε ότι αυτό δεν είναι καθόλου δύσκολο πρόβλημα. Ποτέ δεν χρειάστηκε να σπαταλήσουμε εμείς ή ο υπάλληλος του ταχυδρομείου πολύ χρόνο προκειμένου να επιλεχθούν τα γραμματόσημα εκείνα τα οποία αντιστοιχούν στην αξία του γράμματος. Ο λόγος που το πρόβλημα στο ταχυδρομείο είναι εύκολο οφείλεται στις σχετικά μικρές τιμές τόσο της αξίας του γράμματος, όσο και του πλήθους των διαθέσιμων γραμματοσήμων. Αν το σύνολο των γραμματοσήμων είναι μεγάλο, τότε το πρόβλημα μπορεί να γίνει όντως δύσκολο.

ΠΑΡΑΔΕΙΓΜΑ 6.1 – Επίδειξη δύσκολου προβλήματος των γραμματοσήμων. Έστω ότι το σύνολο των αξιών των γραμματοσήμων είναι το {12, 15, 20, 28, 35, 50, 70, 80, 95, 100, 150, 200} και η αξία του γράμματος είναι 555. Ακόμη και αν απλοποιήσουμε το πρόβλημα υποθέτοντας ότι το σύνολο δεν περιέχει το ίδιο γραμματόσημο πάνω από μια φορά, ο χώρος αναζήτησης αποτελείται από 2^{12} πε-

ριπτώσεις. Παρατηρούμε δηλαδή ότι η πολυπλοκότητα του προβλήματος είναι εκθετική, 2^n. Η λύση είναι το σύνολο {12, 28, 35, 50, 80, 150, 200}.

Ωστόσο, ορίζεται ένα υποσύνολο του προβλήματος του οποίου η λύση είναι εύκολη, ανεξάρτητα από τα μεγέθη του πλήθους των αξιών των γραμματοσήμων και της συνολικής αξίας. Η ύπαρξη του υποσυνόλου αυτού είναι και ο λόγος που το πρόβλημα έχει κρυπτογραφικό ενδιαφέρον. Προκειμένου να καθορίσουμε το εν λόγω υποσύνολο του προβλήματος, θα προχωρήσουμε σε δύο ορισμούς.

ΟΡΙΣΜΟΣ 6.2 – Μια διατεταγμένη ακολουθία ακεραίων (b_1, b_2, …, b_n) ονομάζεται ***γνησίως αύξουσα*** αν:

$$b_{i+1} > b_i , \quad \forall i,\ 1 < i < n .$$

ΟΡΙΣΜΟΣ 6.3 – Μια διατεταγμένη ακολουθία ακεραίων (b_1, b_2, …, b_n) ονομάζεται ***υπεραύξουσα*** αν:

$$b_i > \sum_{j=1}^{i-1} b_j , \quad \forall i,\ 1 < i \le n .$$

Από τους ορισμούς προκύπτει ότι μια υπεραύξουσα ακολουθία είναι και γνησίως αύξουσα, αλλά το αντίστροφο δεν ισχύει. Επομένως, το σύνολο των υπεραυξουσών ακολουθιών είναι υποσύνολο του συνόλου των γνησίως αυξουσών ακολουθιών. Έστω $\boldsymbol{G}$ το σύνολο των γνησίως αυξουσών ακολουθιών και $\boldsymbol{F}$ το σύνολο των υπεραυξουσών ακολουθιών. Όπως είδαμε, $\boldsymbol{F} \subseteq \mathbf{G}$. Είναι φανερό ότι όλες οι περιπτώσεις του προβλήματος του αθροίσματος των γραμματοσήμων μπορούν να εκφραστούν με κάποιο στοιχείο του $\boldsymbol{G}$ και ενός αθροίσματος S.

Θα αποδείξουμε ότι οι περιπτώσεις των προβλημάτων που ανήκουν στο $\boldsymbol{F}$ έχουν εύκολη λύση. Πράγματι, στην περίπτωση της υπεραύξουσας ακολουθίας, υπάρχει αλγόριθμος ο οποίος δοθέντος αθροίσματος S μπορεί να προσδιορίσει τα επιμέρους στοιχεία του αθροίσματος που ανήκουν σε δεδομένη υπεραύξουσα ακολουθία (b_1, b_2, …, b_n). Ο αλγόριθμος είναι ο εξής:

Knapsack(S)

```
1  i ← n, B ← {}
2  repeat
3    if S > b_i then B ← B ∪ {b_i}, S ← S − b_i
4    i ← i − 1
5  until i = 0
6  return B
```

Το βήμα (3) του αλγόριθμου επαναλαμβάνεται n φορές, και κατά τον τερματισμό του το σύνολο B περιέχει τη λύση του προβλήματος. Επομένως η πολυπλοκότητα του αλγόριθμου είναι n.

ΠΑΡΑΔΕΙΓΜΑ 6.2 – Λύση προβλήματος με υπεραύξουσα ακολουθία. Δίνεται η ακολουθία (1, 2, 4, 9, 18, 35, 70) και το άθροισμα 101. Μπορούμε να διαπιστώσουμε ότι η ακολουθία είναι υπεραύξουσα:

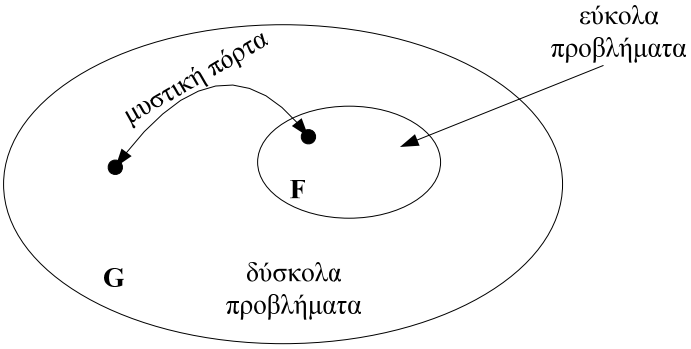
1	< 2
1 + 2 = 3	< 4
1 + 2 + 4 = 7	< 9
1 + 2 + 4 + 9 = 16	< 18
1 + 2 + 4 + 9 + 18 = 34	< 35
1 + 2 + 4 + 9 + 18 + 35 = 69	< 70

Στη συνέχεια εφαρμόζουμε τον αλγόριθμο που περιγράψαμε:

101 – 70 = 31	{70}
31 – 18 = 13	{70, 18}
13 – 9 = 4	{70, 18, 9}
4 = 4	{70, 18, 9, 4}

Μπορούμε να εξακριβώσουμε ότι: 4 + 9 + 18 + 70 = 101.

Το γεγονός ότι υπάρχει ένα σύνολο προβλημάτων ***F*** όπου η λύση είναι εύκολη, ενώ για τα προβλήματα που είναι εκτός του συνόλου ***F*** η λύση είναι δύσκολη, μας οδηγεί στο σχεδιασμό ενός κρυπτοσυστήματος δημόσιου κλειδιού όπως παριστάνεται στο Σχήμα 6.1.



Σχήμα 6.1 Αρχή κρυπτοσυστήματος knapsack

Αρχικά επιλέγουμε ένα εύκολο πρόβλημα. Στη συνέχεια με τη βοήθεια μιας μυστικής πόρτας που γνωρίζουμε μόνον εμείς, αντιστοιχίζουμε το εύκολο πρόβλημα σε κάποιο δύσκολο πρόβλημα. Το εύκολο πρόβλημα και η μυστική πόρτα είναι το ιδιωτικό κλειδί, ενώ το δύσκολο πρόβλημα είναι το δημόσιο κλειδί. Η επιλογή της μυστικής πόρτας έχει άμεσο αντίκτυπο στην επιλογή του δύσκολου προβλήματος. Δηλαδή, αν επιλέξουμε μια δεύτερη μυστική πόρτα, τότε το εύκολο

πρόβλημα θα αντιστοιχισθεί σε ένα δύσκολο πρόβλημα, διαφορετικό από το αρχικό δύσκολο πρόβλημα.

Εφόσον γνωρίζουμε τη μυστική πόρτα μπορούμε με μεγάλη ευκολία να μεταπηδάμε μεταξύ του δύσκολου και του εύκολου προβλήματος. Αυτό ακριβώς είναι και το κρυπτοσύστημα των Merkle και Hellman που περιγράφουμε στη συνέχεια.

6.4.1. Το κρυπτοσύστημα Merkle και Hellman

Οι Merkle και Hellman ανέπτυξαν ένα κρυπτοσύστημα δημόσιου κλειδιού το οποίο βασίζεται στο μετασχηματισμό μιας υπεραύξουσας ακολουθίας σε αύξουσα ακολουθία.

Έστω η υπεραύξουσα ακολουθία (b_1, b_2, …, b_n). Επιλέγουμε modulus m, τέτοιον ώστε:

$$m > \sum_{i=1}^{n} b_i \ .$$

Στη συνέχεια επιλέγουμε ακέραιο w, τέτοιον ώστε $1 < w < m$ και $\gcd(w, m) = 1$, και υπολογίζουμε την ακολουθία $(a'_1, a'_2, ..., a'_n)$ έτσι ώστε:

$$a'_i = wb_i \bmod m$$

Τέλος, αναδιατάσσουμε τα στοιχεία της $(a'_1, a'_2, ..., a'_n)$ κατά αύξουσα διάταξη. Η νέα διάταξη που προκύπτει είναι η (a_1, a_2, …, a_n), η οποία αποτελεί γνησίως αύξουσα ακολουθία (όχι όμως υπεραύξουσα) και αντιστοιχεί σε δύσκολο πρόβλημα.

Από τις παραπάνω παραμέτρους, η (a_1, a_2, …, a_n) είναι το δημόσιο κλειδί, ενώ το σύνολο $\{(b_1, b_2, \ldots, b_n), w, m\}$ είναι το ιδιωτικό κλειδί. Το ζεύγος (w, m) αποτελεί την μυστική πόρτα.

ΠΑΡΑΔΕΙΓΜΑ 6.3 – Δημιουργία παραμέτρων κρυπτοσυστήματος Merkle και Hellman. Έστω η υπεραύξουσα ακολουθία (1, 2, 4, 9, 20, 38). Το άθροισμα όλων των όρων είναι ίσο με 74. Επιλέγουμε $m = 105$. Έστω $w = 31$ ($\gcd(105, 31) = 1$). Υπολογίζουμε την ακολουθία $(a'_1, a'_2, ..., a'_6)$ ως εξής:

$$a'_1 = 1 \times 31 \bmod 105 = 31$$
$$a'_2 = 2 \times 31 \bmod 105 = 62$$
$$a'_3 = 4 \times 31 \bmod 105 = 19$$
$$a'_4 = 9 \times 31 \bmod 105 = 69$$
$$a'_5 = 20 \times 31 \bmod 105 = 95$$
$$a'_6 = 38 \times 31 \bmod 105 = 23$$

Η γνησίως αύξουσα (δύσκολη) ακολουθία που προκύπτει είναι η:

$$(a_1, a_2, a_3, a_4, a_5, a_6) = (19,23,31,62,69,95) = (a'_3, a'_6, a'_1, a'_2, a'_4, a'_5) \ .$$

Η κρυπτογράφηση πραγματοποιείται σε τμήματα απλού κειμένου μεγέθους n bits, όπου n το πλήθος των στοιχείων της ακολουθίας. Έστω $(p_1p_2\ldots p_n)$ το απλό κείμενο εκφρασμένο σε δυαδικά ψηφία. Η κρυπτογράφηση ορίζεται από τη σχέση:

$$c = \sum_{i=1}^{n} p_i a_i \ ,$$

δηλαδή το κρυπτοκείμενο είναι το άθροισμα επιλεγμένων στοιχείων της ακολουθίας, όπου η επιλογή καθορίζεται από τα bits του απλού κειμένου.

ΠΑΡΑΔΕΙΓΜΑ 6.4 – Κρυπτογράφηση κατά Merkle και Hellman. Θα χρησιμοποιήσουμε το κρυπτοσύστημα του Παραδείγματος 6.3 για να κρυπτογραφήσουμε το απλό κείμενο:

$\boldsymbol{P = (001100\ 110100\ 111010)_2}$.

Χωρίζουμε το απλό κείμενο σε τμήματα των 6 bits, όσο είναι και το πλήθος των στοιχείων της ακολουθίας. Κατά την κρυπτογράφηση έχουμε στη διάθεσή μας μόνον το δημόσιο κλειδί, και φυσικά το απλό κείμενο. Η κρυπτογράφηση του $\boldsymbol{P}$ θα δώσει:

$$0\cdot 19 + 0\cdot 23 + 1\cdot 31 + 1\cdot 62 + 0\cdot 69 + 0\cdot 95 = 93$$
$$1\cdot 19 + 1\cdot 23 + 0\cdot 31 + 1\cdot 62 + 0\cdot 69 + 0\cdot 95 = 104$$
$$1\cdot 19 + 1\cdot 23 + 1\cdot 31 + 0\cdot 62 + 1\cdot 69 + 0\cdot 95 = 142 \ .$$

Επομένως το $\boldsymbol{P}$ κρυπτογραφήθηκε στους ακεραίους 93,104,142.

Κατά την αποκρυπτογράφηση, ο κάτοχος του ιδιωτικού κλειδιού μπορεί να μετασχηματίσει το άθροισμα του κρυπτοκειμένου που προέρχεται από τη δύσκολη ακολουθία, στο αντίστοιχο άθροισμα της υπεραύξουσας ακολουθίας. Επειδή το στοιχείο b_i συνδέεται με το στοιχείο a_i' μέσω της σχέσης:

$$a_i' = wb_i \bmod m \ ,$$

έπεται ότι:

$$b_i = w^{-1}a_i' \bmod m \ .$$

Παρόμοια με τα στοιχεία των ακολουθιών, η ίδια σχέση ισχύει και μεταξύ του αθροίσματος C της δύσκολης ακολουθίας, με το άθροισμα D της υπεραύξουσας ακολουθίας:

$$D = w^{-1}C \bmod m \ .$$

Η ανάγκη υπολογισμού του αντιστρόφου του w θέτει την απαίτηση να είναι $\gcd(w,m) = 1$, καθότι στην περίπτωση που τα w και m έχουν κοινούς παράγοντες, ο w^{-1} δεν υπάρχει.

Συνεπώς κατά την αποκρυπτογράφηση, το κρυπτοκείμενο μετασχηματίζεται στο άθροισμα της υπεραύξουσας ακολουθίας, όπου είναι πλέον δυνατή η αποκρυπτογράφησή του.

ΠΑΡΑΔΕΙΓΜΑ 6.5 – Αποκρυπτογράφηση κατά Merkle και Hellman. Ολοκληρώνοντας τα παραπάνω παραδείγματα, θεωρούμε το κρυπτοκείμενο 93,104,142. Ο αντίστροφος του w = 31 mod 105 είναι ο w^{-1} = 61 mod 105 και το κρυπτοκείμενο μετασχηματίζεται στο:

$$93 \cdot 61 \bmod 105 = 3 = 1 + 2\,,$$
$$104 \cdot 61 \bmod 105 = 44 = 2 + 4 + 38\,,$$
$$142 \cdot 61 \bmod 105 = 52 = 1 + 4 + 9 + 38$$

από το οποίο μπορεί να υπολογισθεί το απλό κείμενο, μετά την απομάκρυνση της αναδιάταξης:

$$(a_1, a_2, a_3, a_4, a_5, a_6) = (a'_3, a'_6, a'_1, a'_2, a'_4, a'_5)$$

αρχική ακολουθία:	1	2	4	8	20	38
αναδιάταξη:	4	38	1	2	9	20
Knapsack(3)	0	0	1	1	0	0
Knapsack(44)	1	1	0	1	0	0
Knapsack(52)	1	1	1	0	1	0

Κρυπτανάλυση του κρυπτοσυστήματος Merkle και Hellman

Οι Shamir και Zippel (1980) περιέγραψαν έναν τρόπο εντοπισμού του w, από το δημόσιο κλειδί, υποθέτοντας ότι ο αντίπαλος έχει γνώση του m. Γενικά, λόγω του μετασχηματισμού της υπεραύξουσας ακολουθίας στη δύσκολη, αναμένεται ότι η μέγιστη τιμή της δύσκολης ακολουθίας θα βρίσκεται κοντά στο m, οπότε η διαρροή μιας τέτοιας πληροφορίας είναι αναπόφευχτη.

Έστω ότι τα δύο πρώτα στοιχεία a_1 και a_2 της δύσκολης ακολουθίας αντιστοιχούν στα στοιχεία b_1 και b_2 της εύκολης ακολουθίας. Αν διαιρέσουμε τις σχέσεις μετασχηματισμού μεταξύ τους, θα πάρουμε:

$$l = \frac{a_1}{a_2} = \frac{w\, b_1}{w\, b_2} = \frac{b_1}{b_2} \bmod m$$

Στη συνέχεια αναζητούμε το i για το οποίο η ποσότητα

$$i \cdot l \bmod m\,, \quad 1 \le i \le 2^n$$

ελαχιστοποιείται. Στην περίπτωση αυτή, το i θα είναι ίσο με b_2^{-1}, οπότε θα είναι:

$$i \cdot l = b_1$$

Στη συνέχεια από το b_1 μπορεί να υπολογισθεί το w και επομένως και το w^{-1}.

Εκτός από την κρυπταναλυτική επίθεση των Shamir και Zippel που περιγράψαμε, η βιβλιογραφία περιλαμβάνει και άλλες επιθέσεις (Shamir, 1982, Brickell & Simmons, 1983), με αποτέλεσμα το κρυπτοσύστημα knapsack να μην είναι ασφαλές.

6.5. Το κρυπτοσύστημα RSA

Το κρυπτοσύστημα των Rivest, Shamir, Adleman είναι ένα από τα πιο παλιά και διαδεδομένα κρυπτοσυστήματα δημόσιου κλειδιού. Ιστορικά, η ιδέα του κρυπτοσυστήματος δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, αλλά το πρώτο πρακτικό κρυπτοσύστημα ανακαλύφθηκε το 1977 από τους Rivest, Shamir και Adleman.

Η ασφάλεια του κρυπτοσυστήματος βασίζεται στο δύσκολο πρόβλημα της παραγοντοποίησης ενός σύνθετου ακεραίου σε γινόμενο πρώτων παραγόντων.

ΟΡΙΣΜΟΣ 6.4 – Έστω p και q δύο πρώτοι αριθμοί και $n = pq$. Το κρυπτοσύστημα όπου $\mathcal{P} = \mathcal{C} = \mathbf{Z}_n$,

$$\mathbf{K} = \left\{(p, q, n, k_e, k_d) : k_e k_d \equiv 1 \pmod{\phi(n)}\right\}$$

ορίζει το κρυπτοσύστημα RSA, με πράξη κρυπτογράφησης:

$$e_k(m) = m^{k_e} \bmod n$$

και πράξη αποκρυπτογράφησης:

$$d_k(c) = c^{k_d} \bmod n\ .$$

Το δημόσιο κλειδί αποτελείται από τους ακεραίους k_e και n, ενώ το ιδιωτικό κλειδί αποτελείται από τα p, q, k_d.

Μπορούμε να επαληθεύσουμε ότι η πράξη της αποκρυπτογράφησης δίνει το αρχικό απλό κείμενο ως εξής:

$$c^{k_d} \equiv (m^{k_e})^{k_d} \pmod{n}, \tag{6.1}$$

αλλά επειδή

$$k_e k_d \equiv 1 \pmod{\phi(n)}$$

έπεται ότι

$$k_e k_d = w\phi(n) + 1$$

για κάποια σταθερά $w > 1$. Έτσι η (6.1) γίνεται:

$$c^{k_d} \equiv m^{w\phi(n)} \cdot m \pmod{n}$$

και λόγω του Θεωρήματος του Euler σύμφωνα με το οποίο:

$$m^{\phi(n)} \equiv 1 \pmod{n},$$

θα είναι και

$$\begin{aligned} c^{k_d} &\equiv 1^w \cdot m \pmod{n} \\ &\equiv m \pmod{n} \end{aligned}$$

Παρόμοιο αποτέλεσμα έχουμε και στην περίπτωση όπου ένα κείμενο κρυπτογραφείται με k_d και αποκρυπτογραφείται με k_e. Η αντιμεταθετική ιδιότητα που ισχύει στο εκθετικό γινόμενο έχει ως αποτέλεσμα και οι πράξεις της κρυπτογράφησης και αποκρυπτογράφησης να είναι αμοιβαία αντίστροφες, δηλαδή:

$$p = c^{k_d} \equiv (m^{k_e})^{k_d} \equiv (m^{k_d})^{k_e} \pmod{n}.$$

ΠΑΡΑΔΕΙΓΜΑ 6.6 – Κρυπτογράφηση κατά RSA. Θα κατασκευάσουμε ένα κρυπτοσύστημα RSA με μικρές παραμέτρους. Έστω $p = 11$ και $q = 29$, οπότε θα είναι:

$$n = 11 \times 29 = 319, \quad \phi(n) = 10 \times 28 = 280.$$

Για δημόσιο κλειδί επιλέγουμε $k_e = 101$ και με βάση αυτό υπολογίζουμε το ιδιωτικό κλειδί:

$$k_e \cdot k_d \equiv 1 \pmod{\phi(n)},$$

δηλαδή:

$$k_d = 61.$$

Προκειμένου να κρυπτογραφήσουμε ένα μήνυμα, θα πρέπει αρχικά να αντιστοιχίσουμε (ή ισοδύναμα να κωδικοποιήσουμε) τα σύμβολα του απλού κειμένου στο σύνολο $\boldsymbol{Z}_{319}$. Έστω το μήνυμα [ρεμα]. Ορίζουμε την αντιστοίχιση $\text{Α} \mapsto 10$, $\text{Β} \mapsto 11$, …, $\Omega \mapsto 33$. Διαλέξαμε τη συγκεκριμένη αντιστοίχιση ώστε όλα τα σύμβολα του απλού κειμένου να κωδικοποιούνται με σταθερό πλήθος ψηφίων, για να μην υπάρχουν ασάφειες στην αποκωδικοποίηση. Συνεπώς το αριθμητικό ισοδύναμο μήνυμα είναι το [26 14 21 10]. Στη συνέχεια ομαδοποιούμε τα ψηφία έτσι ώστε οι αριθμοί που δημιουργούνται να είναι μικρότεροι του δημόσιου modulus: (261, 42, 110). Η κρυπτογραφική πράξη εφαρμόζεται τρεις φορές:

$261^{101} = 261 \bmod 319$
$42^{101} = 196 \bmod 319$
$110^{101} = 132 \bmod 319$

Δηλαδή το κρυπτοκείμενο είναι το (261, 196, 132). Παρατηρούμε ότι η κρυπτογράφηση του 261 είναι ο εαυτός του. Για RSA με μεγάλες παραμέτρους, το φαι-

νόμενο αυτό έχει μικρή πιθανότητα να συμβεί. Ωστόσο, ο αντίπαλος μπορεί να εντοπίσει σε ένα κρυπτογραφημένο μήνυμα ποια τμήματα δεν έχουν ουσιαστικά κρυπτογραφηθεί, εφαρμόζοντας μόνο το δημόσιο κλειδί.

6.5.1. Ανάλυση του RSA

Η πρακτική αξία του RSA οφείλεται στο γεγονός ότι αφενός μεν δεν υπάρχει αλγόριθμος ο οποίος να εντοπίζει τους πρώτους παράγοντες ενός σύνθετου ακεραίου, αφετέρου δε ο υπολογισμός μεγάλης δύναμης ενός αριθμού σε modular αριθμητική μπορεί να γίνει σε επιτρεπτό (γραμμικό) χρόνο.

Η πρώτη παρατήρηση αφορά την ασφάλεια του κρυπταλγόριθμου. Οι πρώτοι αριθμοί p και q θα πρέπει να είναι αρκετά μεγάλοι, ώστε ο καλύτερος γνωστός αλγόριθμος παραγοντοποίησης να απαιτεί χρόνο μεγαλύτερο από αυτόν με τον οποίο πρέπει να προστατευθούν τα δεδομένα. Στον Πίνακα 6.1 παρουσιάζονται ενδεικτικά μεγέθη και αντίστοιχες περιπτώσεις στις οποίες θα πρέπει να εφαρμοσθούν τα μεγέθη αυτά.

p, q	n	χρόνος προστασίας	τύπος δεδομένων
256 bits	512 bits	μερικές εβδομάδες	πληροφορίες που επηρεάζουν βραχυπρόθεσμα το χρηματιστήριο (π.χ. απόφαση συγχώνευσης δύο εταιρειών)
512 bits	1024 bits	50-100 χρόνια	προσωπικά μυστικά
1024 bits	2048 bits	>100 χρόνια	εμπορικά μυστικά, προσωπικά δεδομένα
2048 bits	4096 bits	≈ ηλικία του Σύμπαντος	στρατιωτικά μυστικά

Πίνακας 6.1 Μεγέθη παραμέτρων RSA και ενδεικτικοί τύποι δεδομένων προς προστασία

Όσον αφορά τον υπολογισμό της ύψωσης ακεραίου σε δύναμη, ο αλγόριθμος «*επαναλαμβανόμενου τετραγωνισμού – και – πολλαπλασιασμού*» (βλ. § 2.7) είναι αποτελεσματικός, αφού η πολυπλοκότητά του είναι (γραμμικώς) ανάλογη με το μέγεθος των ακεραίων που λαμβάνουν μέρος στην εκθετική πράξη.

Η συνάρτηση ύψωσης ακεραίου σε δύναμη

Θεωρούμε την οικογένεια συναρτήσεων $f_a(x) = x^a \bmod n$, για δεδομένο ακέραιο n. Η συνάρτηση αυτή ορίζει τη βασική κρυπτογραφική πράξη του κρυπτοσυστήματος RSA (όπου n το γινόμενο δύο πρώτων). Η συνάρτηση είναι περιοδική ως προς τον εκθέτη a.

Ας εξετάσουμε αρχικά την περίπτωση $n = p$, όπου p είναι πρώτος. Στον Πίνακα 6.2 παρουσιάζονται τα αποτελέσματα της συνάρτησης για $0 < x < p$, $p = 17$. Ο εκθέτης a είναι διατεταγμένος κατά γραμμές.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1
3	1	8	10	13	6	12	3	2	15	14	5	11	4	7	9	16
4	1	16	13	1	13	4	4	16	16	4	4	13	1	13	16	1
5	1	15	5	4	14	7	11	9	8	6	10	3	13	12	2	16
6	1	13	15	16	2	8	9	4	4	9	8	2	16	15	13	1
7	1	9	11	13	10	14	12	15	2	5	3	7	4	6	8	16
8	1	1	16	1	16	16	16	1	1	16	16	16	1	16	1	1
9	1	2	14	4	12	11	10	8	9	7	6	5	13	3	15	16
10	1	4	8	16	9	15	2	13	13	2	15	9	16	8	4	1
11	1	8	7	13	11	5	14	2	15	3	12	6	4	10	9	16
12	1	16	4	1	4	13	13	16	16	13	13	4	1	4	16	1
13	1	15	12	4	3	10	6	9	8	11	7	14	13	5	2	16
14	1	13	2	16	15	9	8	4	4	8	9	15	16	2	13	1
15	1	9	6	13	7	3	5	15	2	12	14	10	4	11	8	16
16	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
17	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Πίνακας 6.2 Τιμές της $f_a(x)$ mod 17

Από τον παραπάνω πίνακα παρατηρούμε ότι $5^{11} = 11 \bmod 17$ και $11^3 = 5 \bmod 17$. Επίσης παρατηρούμε ότι $7^{11} = 14 \bmod 17$ και $14^3 = 7 \bmod 17$. Γενικά μπορούμε να διαπιστώσουμε ότι αν $x^{11} = y \bmod 17$, τότε $y^3 = x \bmod 17$, ή ισοδύναμα, ότι η $f_{11}(x)$ είναι η αντίστροφη της $f_3(x)$.

Οι αντίστροφες σχέσεις, modulo 17, του 3 και 11, μπορούν να επαληθευτούν με το θεώρημα του Fermat. Για δεδομένο x, είναι:

$$x^{11\cdot 3} \equiv x^{33} \equiv x \pmod{17},$$

λόγω του ότι

$$x^{17-1} \equiv 1 \pmod{17}$$

οπότε και

$$x^{33} \equiv x^{32}\cdot x \equiv (x^{17-1})^2\cdot x \equiv 1^2\cdot x \equiv x \pmod{17}.$$

Από τις συναρτήσεις $f_a(x)$, μας ενδιαφέρουν αυτές οι οποίες είναι αντιστρέψιμες. Για παράδειγμα, στον παραπάνω πίνακα η $f_2(x)$ δεν είναι αντιστρέψιμη, διότι $f_2(8) = f_2(9) = 13$. Οι δυνάμεις εκείνες οι οποίες ορίζουν αντιστρέψιμες συναρτήσεις είναι εκείνες που δεν έχουν κοινούς παράγοντες με τον $p - 1$, στην περίπτωσή μας με τον 16. Το $p - 1$ προκύπτει από το Θεώρημα του Fermat, όπου μπορούμε να

παρατηρήσουμε ότι οι πράξεις στους εκθέτες γίνονται ουσιαστικά modulo $(p - 1)$. Έτσι δύο συναρτήσεις $f_a(x)$ και $f_b(x)$ είναι αντίστροφες, αν

$$a \cdot b \equiv 1 \bmod (p - 1).$$

Είναι φανερό ότι δοθέντων a και p, είναι εύκολο να βρεθεί ο $a^{-1} = b$, με τον αλγόριθμο του Ευκλείδη στην ανεπτυγμένη του μορφή (βλ. § 2.4).

Λόγω του ότι για να υπολογισθεί η modular δύναμη ενός ακεραίου θα πρέπει να είναι γνωστό το modulus, οι συναρτήσεις $f_a(x) \bmod n$ δεν έχουν κρυπτογραφικό ενδιαφέρον όταν το n είναι πρώτος αριθμός, διότι λόγω του Θεωρήματος του Fermat ο υπολογισμός του αντιστρόφου του εκθέτη είναι εύκολος. Έτσι εξετάζουμε την περίπτωση όπου το n είναι σύνθετος ακέραιος και για την ακρίβεια είναι γινόμενο δύο πρώτων.

Στον Πίνακα 6.3 έχουν υπολογισθεί οι τιμές της $f_a(x) \bmod 15$**.** Γνωρίζουμε ότι $15 = 3 \cdot 5$.

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

Πίνακας 6.3 Τιμές της $f_a(x) \bmod 15$

Παρατηρούμε ότι η συνάρτηση είναι περιοδική ως προς τον εκθέτη, με μέγιστη περίοδο T = 4, να συμβαίνει για $f_a(2), f_a(3), f_a(7), f_a(12), f_a(13)$. Για οποιαδήποτε x $(x \neq 0)$ και a θα είναι:

$$f_a(x) \equiv f_{a+T}(x) \pmod{n}$$

ή ισοδύναμα:

$$x^{T+1} \equiv x \pmod{n}.$$

Από την παραπάνω σχέση προκύπτει ότι για δύο εκθέτες a και b οι οποίοι ορίζουν αντίστροφες συναρτήσεις θα πρέπει να ισχύει:

$$a \cdot b \equiv 1 \bmod (T).$$

Για n γινόμενο δύο πρώτων p και q, η περίοδος υπολογίζεται εύκολα από τη σχέση:

$$T = \text{lcm}(p - 1, q - 1),$$

όπου lcm( ) το ελάχιστο κοινό πολλαπλάσιο. Συνεπώς, η περίοδος δεν μπορεί να υπολογισθεί αν δεν είναι γνωστοί οι παράγοντες p και q του n και κατ' επέκταση δοθέντος εκθέτη a, δεν μπορεί να υπολογισθεί αποτελεσματικά ο αντίστροφος b, για μεγάλους p και q. Σε αυτήν την παρατήρηση στηρίζεται η ασφάλεια του RSA.

Επίσης, προκειμένου να ορίζεται η αντίστροφη της $f_a(x) \bmod n$, θα πρέπει ο εκθέτης να ορίζει ενριπτική συνάρτηση. Παρόμοια με την $f_a(x) \bmod p$, όπου ο εκθέτης θα πρέπει να μην έχει κοινούς παράγοντες με τον p, στην περίπτωση της $f_a(x) \bmod n$, ο εκθέτης θα πρέπει να μην έχει κοινούς παράγοντες με τον $(p - 1)$ και τον $(q - 1)$.

Από τους εκθέτες a και $b = a^{-1} \bmod T$, λόγω της αντιμεταθετικότητας, μπορεί οποιοσδήποτε να επιλεχθεί ως δημόσιο κλειδί, οπότε ο άλλος θα θεωρηθεί ιδιωτικό κλειδί. Ωστόσο, για την αποφυγή εξαντλητικής αναζήτησης προτιμάται ο μικρότερος από τους δύο να είναι το δημόσιο κλειδί και ο μεγαλύτερος το ιδιωτικό κλειδί.

Σχέση μεταξύ lcm(p–1, q–1) και $\phi(n)$

Στην παραπάνω ανάλυση της συνάρτησης ύψωσης σε εκθέτη υπολογίσαμε το ελάχιστο κοινό πολλαπλάσιο μεταξύ των (p–1) και (q–1), ενώ στον ορισμό του κρυπτοσυστήματος RSA η αντίστοιχη πράξη είναι η $\phi(n)$. Η εναλλαγή των δύο αυτών όρων έγινε προς χάριν απλούστευσης της παρουσίασης, ενώ η διατήρηση της $\phi(n)$ στον ορισμό του RSA έγινε για να συμφωνούμε με την διατύπωση του RSA από τους δημιουργούς του.

Η ποσότητα lcm(p–1, q–1) ονομάζεται συνάρτηση Carmichael και συμβολίζεται με $\psi(n)$. Η $\psi(n)$ είναι διαιρέτης της $\phi(n)$, δηλαδή:

$$\phi(n) = c \cdot \psi(n),$$

για κάποιον ακέραιο c. Έτσι κατ' επέκταση, για δεδομένο a, με gcd(a ,n) = 1, ισχύει:

$$a^{\psi(n)} \equiv 1 \pmod{n}.$$

Αυτό είναι γνωστό ως Θεώρημα του Carmichael και είναι γενίκευση του θεωρήματος του Euler.

Μια χρήσιμη σχέση μεταξύ της συνάρτησης Carmichael και των παραγόντων του n, την οποία θα χρησιμοποιήσουμε για επίθεση στον RSA είναι η:

$$\psi(n) = \psi(p \cdot q) = 2 \cdot lcm\left(\frac{p-1}{2}, \frac{q-1}{2}\right),$$

η οποία προκύπτει από τις:

$$\psi(2 \cdot p \cdot q) = lcm(2-1, p-1, q-1) = lcm(p-1, q-1).$$

6.5.2. Ασφάλεια του RSA

Αν και ο RSA θεωρείται ασφαλής κρυπταλγόριθμος για μεγάλες παραμέτρους, υπάρχουν ορισμένες απειλές που οφείλονται κυρίως στην μη προσεκτική υλοποίηση και εκτέλεση του κρυπτοσυστήματος. Θα πρέπει επίσης να αναφέρουμε ότι ο ισχυρισμός που θέσαμε παραπάνω σχετικά με την ασφάλεια του RSA και τη δυσκολία παραγοντοποίησης ενός σύνθετου ακεραίου, δεν είναι απόλυτα σωστός, με την έννοια ότι δεν έχει αποδειχθεί ότι η ασφάλεια του RSA εξαρτάται αποκλειστικά από την παραγοντοποίηση των ακεραίων. Βέβαια, στην περίπτωση που ανακαλυφθεί αλγόριθμος ο οποίος μπορεί να παραγοντοποιεί σε πολυωνυμικό χρόνο έναν ακέραιο, το RSA δεν είναι ασφαλές.

Το αντίστροφο όμως δεν είναι αληθές. Όπως θα δείξουμε στη συνέχεια, υπάρχουν επιθέσεις οι οποίες μπορούν να προσβάλλουν ένα κρυπτοσύστημα RSA, όπου δεν απαιτείται γνώση των παραγόντων του n.

Επίθεση σε κοινό modulus

Η επίθεση σε κοινό modulus μπορεί να εφαρμοσθεί σε περιπτώσεις όπου υπάρχει μια ομάδα επικοινωνούντων που έχουν κλειδιά των οποίων το n είναι το ίδιο.

Έστω ένα απλό κείμενο m και δύο ζευγάρια κλειδιών (e_1, d_1) και (e_2, d_2) τα οποία έχουν κοινό modulus, n. Η κρυπτογράφηση του απλού κειμένου με τα δύο δημόσια κλειδιά θα δώσει αντίστοιχα:

$$c_1 = m^{e_1} \bmod n, \text{ και}$$

$$c_2 = m^{e_2} \bmod n.$$

Αν $\gcd(e_1, e_2) = 1$, τότε υπάρχουν ακέραιοι w και v, τέτοιοι ώστε:

$$we_1 + ve_2 = 1.$$

Επειδή όμως είναι $e_1, e_2 > 0$, έπεται ότι κάποιο από τα w και v είναι αρνητικό και το άλλο είναι θετικό. Έστω ότι $w < 0$. Τότε ο αντίπαλος έχοντας γνώση των κρυπτοκειμένων και των δημόσιων κλειδιών, μπορεί να ανακτήσει το μήνυμα υπολογίζοντας:

$$(c_1^{-1})^{-w} \cdot c_2^{v} \equiv m^{we_1 + ve_2} \equiv m \pmod n$$

Η επίθεση είναι δυνατή σε περιπτώσεις ομάδας χρηστών όπου η δημιουργία των κλειδιών γίνεται από ένα κέντρο δημιουργίας κλειδιών το οποίο χρησιμοποιεί την ίδια διαδικασία για την δημιουργία των κλειδιών των μελών της ομάδας. Η κρυπτογράφηση ενός μηνύματος με περισσότερα από ένα δημόσια κλειδιά εμφανίζε-

ται σε περιπτώσεις εκπομπής (broadcast), όπου μια οντότητα στέλνει το μήνυμα σε πολλούς αποδέκτες.

Επίθεση επαναληπτικής κρυπτογράφησης

Η επίθεση με κοινό modulus είναι επίθεση η οποία εκμεταλλεύεται συγκεκριμένη υλοποίηση του RSA, η οποία μπορεί να συμβεί σε μοντέλα επικοινωνίας του «ενός προς πολλούς» (one-to-many communication). Αντίθετα, η επίθεση της επαναληπτικής κρυπτογράφησης μπορεί να εφαρμοσθεί σε οποιαδήποτε περίπτωση.

Η επίθεση βασίζεται στην ιδιότητα της περιοδικότητας της συνάρτησης του κρυπτοσυστήματος RSA. Έστω (*e, n*) το δημόσιο κλειδί του Βύρωνα. Η Αλίκη κρυπτογραφεί ένα μήνυμα *m* με την κρυπτογραφική πράξη του RSA:

$$c = m^e \bmod n .$$

Θα συμβολίζουμε με $c^{(0)}$ το κρυπτοκείμενο που προκύπτει από την κρυπτογράφηση του *m* με το δημόσιο κλειδί (*e, n*). Ο αντίπαλος έχοντας συλλάβει το $c^{(0)}$, εκτελεί διαδοχικά κρυπτογραφήσεις:

$$c^{(i)} \equiv (c^{(i-1)})^e \pmod n, \text{ για } i = 1,2,3,...$$

Λόγω της περιοδικότητας, για κάποιο $i = k$, θα είναι:

$$c^{(k)} \equiv (c^{(k-1)})^e \equiv m \pmod n .$$

Σε αυτό το στάδιο ο αντίπαλος δεν είναι σε θέση να γνωρίζει ότι το μήνυμα της Αλίκης είναι το $c^{(k)}$. Αυτό το διαπιστώνει στην επόμενη επανάληψη:

$$c^{(k+1)} \equiv (m)^e \equiv c \pmod n .$$

Η τιμή του *k* για την οποία καταλήγουμε στο αρχικό μήνυμα, ονομάζεται ***εκθέτης ανάκτησης*** (recovery exponent). Είναι προφανές ότι προκειμένου η επίθεση επαναληπτικής κρυπτογράφησης να είναι πρακτικώς αδύνατη, θα πρέπει ο εκθέτης ανάκτησης να είναι όσο το δυνατό μεγαλύτερος. Δυστυχώς λόγω της περιοδικότητας, ο εκθέτης ανάκτησης έχει ένα ανώτατο όριο. Χρησιμοποιώντας το θεώρημα του Carmichael, μπορούμε να υπολογίσουμε το άνω όριο του εκθέτη ανάκτησης, ως εξής:

$$\begin{aligned} c^{(i)} &\equiv m^{e^i} \pmod n \\ &\equiv m^{e^i \bmod \psi(n)} \pmod n \\ &\equiv m^{e^{i \bmod \psi(\psi(n))}} \pmod n \end{aligned}$$

Για να πάρουμε το *m*, θα πρέπει ο εκθέτης του *e* να είναι ίσος με μηδέν, οπότε και $e^0 = 1$. Αυτό συμβαίνει για την τιμή όπου:

$$k = i = \psi(\psi(n)).$$

Επομένως, για να είναι η επίθεση επαναληπτικής κρυπτογράφησης πρακτικά αδύνατη, απαιτείται η τιμή του $\psi(\psi(n))$ να είναι όσο το δυνατόν μεγαλύτερη. Από τη σχέση:

$$\psi(n) = \psi(p \cdot q) = 2 \cdot lcm\left(\frac{p-1}{2}, \frac{q-1}{2}\right)$$

μπορούμε να καταλήξουμε στις ακόλουθες απαιτήσεις, προκειμένου να είναι τουλάχιστον η $\psi(n)$ σχετικά μεγάλη:

- οι ποσότητες $(p–1)/2$ και $(q–1)/2$ θα πρέπει να περιέχουν μεγάλους παράγοντες,
- ο μέγιστος κοινός διαιρέτης των $(p–1)/2$ και $(q–1)/2$ να είναι μικρός.

Η πρώτη σχέση απαιτείται λόγω της διπλής εφαρμογής της συνάρτησης $\psi(\ )$, οπότε κατά τη δεύτερη εφαρμογή της $\psi(\ )$ οι παράγοντες των δύο λόγων θα επηρεάσουν σημαντικά το μέγεθος του αποτελέσματος. Η δεύτερη σχέση απαιτείται λόγω της αντίστροφης σχέσης μεταξύ του μέγιστου κοινού διαιρέτη και του ελάχιστου κοινού πολλαπλασίου. Ιδανικά, οι παραπάνω τιμές είναι βέλτιστες όταν οι p και q είναι ***ασφαλείς πρώτοι***, όταν δηλαδή οι ποσότητες $(p–1)/2$ και $(q–1)/2$ είναι επίσης πρώτοι.

6.6. Το κρυπτοσύστημα ElGamal

Η ασφάλεια του κρυπτοσυστήματος ElGamal βασίζεται στο πρόβλημα του Διακριτού Λογάριθμου.

ΟΡΙΣΜΟΣ 6.5 – Έστω p ένας πρώτος. Το κρυπτοσύστημα το οποίο ορίζεται από $\mathcal{F} = \boldsymbol{Z}_p^*$, $\mathcal{G} = \boldsymbol{Z}_p^* \times \boldsymbol{Z}_p^*$ και $\boldsymbol{K} = \{(p, s, a, b): b = s^a \bmod p\}$, όπου $s \in \boldsymbol{Z}_p^*$, είναι γεννήτορας του $\boldsymbol{Z}_p^*$, ορίζει το κρυπτοσύστημα ElGamal με πράξη κρυπτογράφησης:

$$e_k(m, r) = (y_1, y_2),$$

όπου $r \in Z_{p-1}^*$ τυχαίος ακέραιος,

$$y_1 = s^r \bmod p$$

και

$$y_2 = mb^r \bmod p.$$

Η πράξη αποκρυπτογράφησης ορίζεται για $c = (y_1, y_2)$, $y_1, y_2 \in Z_p^*$:

$$d_k(y_1, y_2) = y_2 (y_1^a)^{-1} \bmod p .$$

Το δημόσιο κλειδί του κρυπτοσυστήματος είναι τα (p, s, b), ενώ το ιδιωτικό κλειδί είναι το a. Η αποκρυπτογράφηση είναι δυνατή διότι:

$$d_k(y_1, y_2) \equiv y_2 (y_1^a)^{-1} \equiv m b^r (s^{ar})^{-1} \equiv m b^r (b^r)^{-1} \equiv m \pmod p .$$

6.6.1. Ασφάλεια του ElGamal

Ο αντίπαλος που θα επιχειρήσει επίθεση στο κρυπτοσύστημα, θα πρέπει να ανακτήσει το ιδιωτικό κλειδί a, από τη σχέση:

$$b = s^a \bmod p ,$$

γνωρίζοντας τα p, s, b. Θα πρέπει δηλαδή να λύσει το διακριτό λογάριθμο με βάση s. Ωστόσο, θεωρούμε ότι η ασφάλεια του κρυπτοσυστήματος ElGamal βασίζεται στο διακριτό λογάριθμο, διότι η λύση του διακριτού λογάριθμου μπορεί να καθιστά το κρυπτοσύστημα ανασφαλές, αλλά δεν έχει αποδειχθεί το αντίστροφο, ότι δηλαδή η ασφάλεια του κρυπτοσυστήματος στηρίζεται αποκλειστικά στο πρόβλημα του διακριτού λογάριθμου.

Η ύπαρξη του τυχαίου αριθμού r, έχει ως αποτέλεσμα τη δυνατότητα αντιστοίχισης του απλού κειμένου σε p–1 κρυπτοκείμενα. Η διαδικασία όπου το απλό κείμενο αναμειγνύεται με μια τυχαία μεταβλητή, ονομάζεται ***διαδικασία δημιουργίας συνθηκών τυχαιότητας*** (randomization process). Το βήμα αυτό το οποίο δεν υπάρχει στο RSA, καθιστά το κρυπτοσύστημα ElGamal ανθεκτικότερο σε επιθέσεις παρόμοιες με αυτές που παρουσιάστηκαν για το RSA. Βέβαια, η χρήση του τυχαίου αριθμού εισάγει έναν επιπλέον κίνδυνο που οδηγεί σε μια πρόσθετη απαίτηση. Για κάθε μήνυμα που κρυπτογραφείται, θα πρέπει να επιλέγεται διαφορετικός τυχαίος r. Στην περίπτωση που δύο μηνύματα m και m' κρυπτογραφηθούν με τον ίδιο r, τότε για τα αντίστοιχα κρυπτοκείμενα που θα προκύψουν (y_1, y_2) και (y_1', y_2'), η γνώση του ενός μηνύματος επιτρέπει την ανάκτηση του άλλου από τον λόγο:

$$\frac{y_2}{y_2'} = \frac{m b^r}{m' b^r} = \frac{m}{m'} .$$

Τέλος, όσον αφορά το μέγεθος του p, το κατώτατο όριο που προτείνεται είναι 1024 bits. Γενικά, κατά την κρυπτογράφηση με το κρυπτοσύστημα ElGamal, το μέγεθος των παραμέτρων αποτελεί σημαντικό κριτήριο υλοποίησης, λόγω του αυξημένου χρόνου που απαιτείται για την κρυπτογράφηση (δύο πράξεις ύψωσης σε δύναμη έναντι της μιας στην περίπτωση του RSA), και λόγω της διαστολής του κρυπτοκειμένου. Τα μειονεκτήματα αυτά έχουν σαν αποτέλεσμα να προτιμάται μειωμένο μέγεθος του modulus.

6.7. Κρυπτοσυστήματα ελλειπτικών καμπυλών

Τα κρυπτοσυστήματα ελλειπτικών καμπυλών δεν είναι νέα κρυπτοσυστήματα. Οι ελλειπτικές καμπύλες αποτελούν ένα μαθηματικό εργαλείο με το οποίο μπορούν να υλοποιηθούν γνωστά κρυπτοσυστήματα δημόσιου κλειδιού. Η εφαρμογή των ελλειπτικών καμπυλών στην κρυπτογραφία προτάθηκε από τους Miller (1986) και Koblitz (1987), ανεξάρτητα.

Οι ελλειπτικές καμπύλες μπορούν να ορισθούν σε διάφορα σώματα, όπως στο σώμα των πραγματικών, των μιγαδικών, κτλ. Ειδικότερα στην κρυπτογραφία, οι ελλειπτικές καμπύλες ορίζονται σε πεπερασμένα σώματα.

Προτού προχωρήσουμε στις ελλειπτικές καμπύλες που είναι ορισμένες σε πεπερασμένα σώματα, θα παρουσιάσουμε ορισμένες ελλειπτικές καμπύλες στο σώμα των πραγματικών αριθμών, προκειμένου να αντιληφθούμε τη μορφή τους και τις ιδιότητές τους.

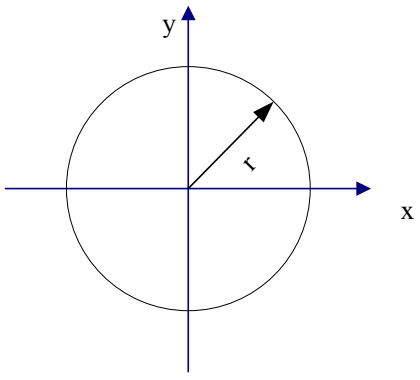
6.7.1. Ελλειπτικές καμπύλες στο σώμα των πραγματικών αριθμών

Αντίθετα από την αίσθηση που μας δημιουργεί ο όρος «καμπύλη», μια ελλειπτική καμπύλη μπορεί να αποτελείται στην πραγματικότητα από δύο καμπύλες και ένα σημείο που βρίσκεται εκτός των καμπυλών.

Ξεκινώντας από την εξίσωση του κύκλου, θα προσθέσουμε διαδοχικά όρους έως ότου καταλήξουμε στην εξίσωση της ελλειπτικής καμπύλης. Όπως είναι γνωστό από την Αναλυτική Γεωμετρία, ένας κύκλος με κέντρο O(0, 0) ορίζεται από την εξίσωση:

$$x^2 + y^2 = r^2,$$

όπου r η ακτίνα του κύκλου. Αν απεικονίσουμε όλα τα σημεία (x, y) ενός επιπέδου τα οποία ικανοποιούν την εξίσωση του κύκλου, θα πάρουμε την κυκλική καμπύλη όπως φαίνεται στο Σχήμα 6.2.

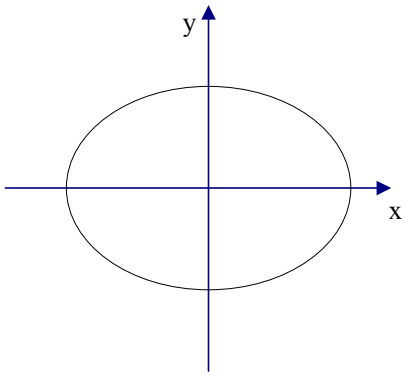


Σχήμα 6.2 $x^2 + y^2 = r^2$ στους πραγματικούς αριθμούς

Ο κύκλος είναι ειδική περίπτωση έλλειψης, όπου $a = b$:

$$ax^2 + by^2 = c$$

Οι τιμές οι οποίες ικανοποιούν την εξίσωση έλλειψης για δοσμένα a και b σχηματίζουν την καμπύλη του Σχήματος 6.3.



Σχήμα 6.3 $ax^2 + by^2 = c$ στους πραγματικούς αριθμούς

Τόσο στην εξίσωση κύκλου, όσο και στην εξίσωση έλλειψης, οι μεταβλητές συνδέονται με δευτεροβάθμιες εξισώσεις. Αυτό έχει σαν αποτέλεσμα σε μια δοσμένη τιμή του x να αντιστοιχούν δύο τιμές για το y, και αντίστροφα. Για δοσμένα διαφορετικά σημεία (x_1, y_1) και (x_2, y_2) της έλλειψης μπορεί να ορισθεί ευθεία η οποία περνά από τα σημεία αυτά. Η ευθεία θα τέμνει την έλλειψη μόνον σε αυτά τα δύο σημεία.

Στην περίπτωση της ελλειπτικής καμπύλης, η εξίσωση της καμπύλης είναι δευτεροβάθμια ως προς y αλλά τριτοβάθμια ως προς x. Η εξίσωση της ελλειπτικής καμπύλης δίνεται από τη σχέση:

$$y^2 = x^3 + ax + b\ ,$$

για σταθερές a και b. Θεωρούμε δύο διαφορετικά σημεία (x_1, y_1) και (x_2, y_2) της ελλειπτικής καμπύλης, και έστω η ευθεία

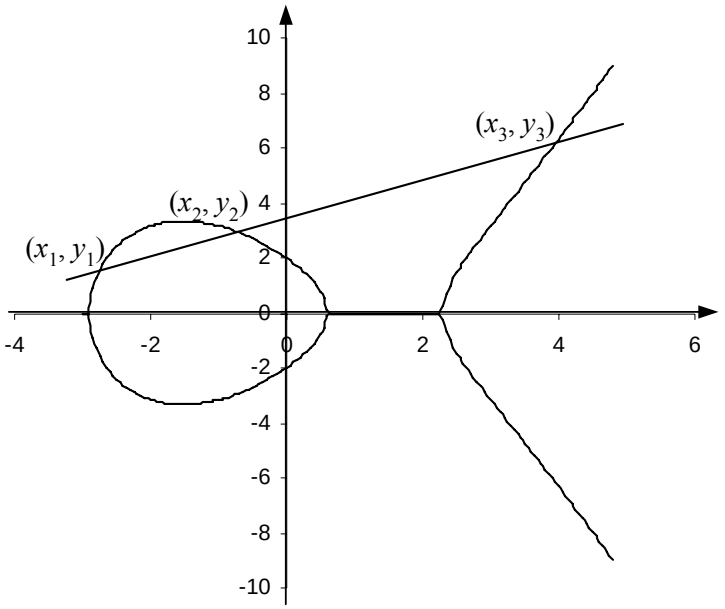
$$y = \lambda x + c$$

η οποία τέμνει την ελλειπτική καμπύλη στα σημεία αυτά. Αντικαθιστώντας την εξίσωση της ευθείας στην ελλειπτική καμπύλη, θα είναι:

$$(\lambda x + c)^2 = x^3 + ax + b\ ,$$

η οποία είναι τριτοβάθμια εξίσωση με δύο από τις ρίζες τα x_1 και x_2. Υπάρχει όμως και η τρίτη ρίζα x_3, που αντιστοιχεί στο σημείο της ευθείας $(x_3, \lambda x_3 + c)$. Συνεπώς η ευθεία τέμνει στην καμπύλη σε τρία σημεία.

Στο Σχήμα 6.4 απεικονίζεται μια ελλειπτική καμπύλη και η ευθεία που τέμνει την καμπύλη σε τρία σημεία. Η ελλειπτική καμπύλη αποτελείται από τις καμπύλες του σχήματος και επιπλέον από ένα σημείου **O** που το ονομάζουμε «σημείο στο άπειρο» (point at infinity).

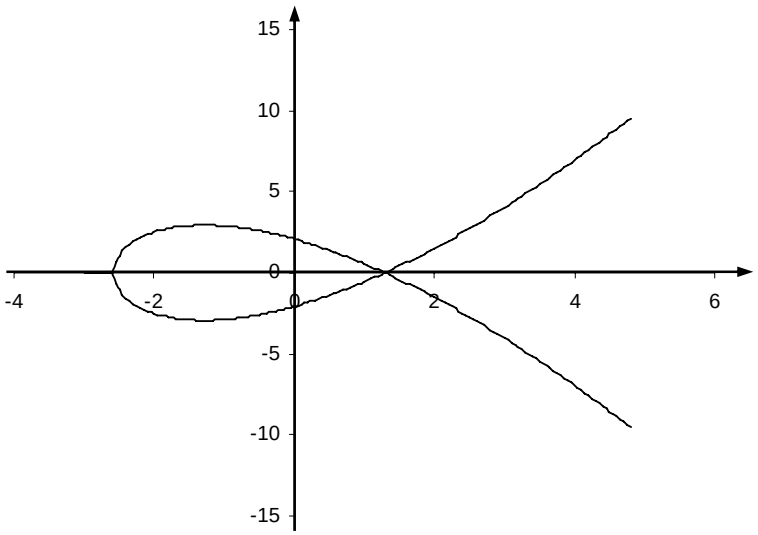


Σχήμα 6.4 Η ελλειπτική καμπύλη $y^2 = x^3 - 7x + 4$

Για κάποιον συνδυασμό των a και b, η εξίσωση της ελλειπτικής καμπύλης δεν έχει τρεις διαφορετικές ρίζες (για $y = 0$). Αυτό συμβαίνει όταν

$$4a^3 + 27b^2 = 0$$

και η ελλειπτική καμπύλη είναι της μορφής του Σχήματος 6.5. Μια τέτοια ελλειπτική καμπύλη ονομάζεται ***ιδιάζουσα*** (singular).

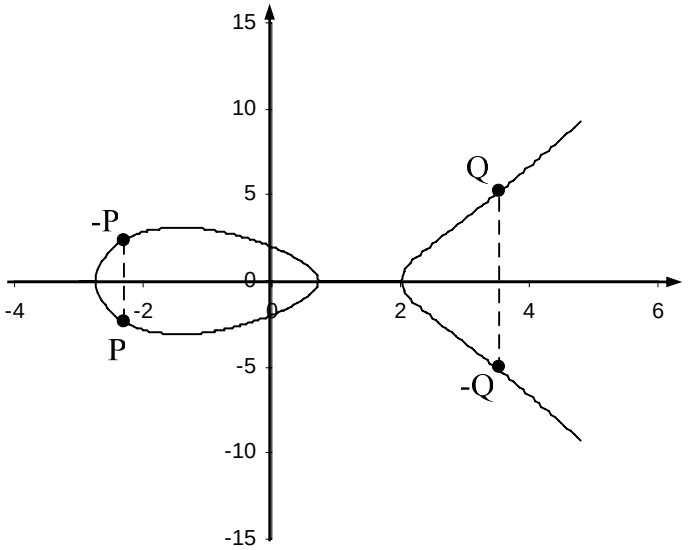


Σχήμα 6.5 Singular ελλειπτική καμπύλη

Πρόσθεση σημείων ελλειπτικής καμπύλης

Αρχικά θα παρουσιάσουμε πως ορίζεται γραφικά η πρόσθεση σημείων ελλειπτικής καμπύλης. Η πρόσθεση βασίζεται στο γεγονός ότι μια ευθεία μπορεί να τέμνει μια ελλειπτική καμπύλη σε τρία το πολύ σημεία.

Αν εξετάσουμε μια ελλειπτική καμπύλη θα διαπιστώσουμε ότι αυτή είναι συμμετρική ως προς τον άξονα x. Έτσι μπορούμε να ορίσουμε το αντίθετο σημείο (–P) ενός σημείου (P) της καμπύλης όπως φαίνεται στο Σχήμα 6.6.



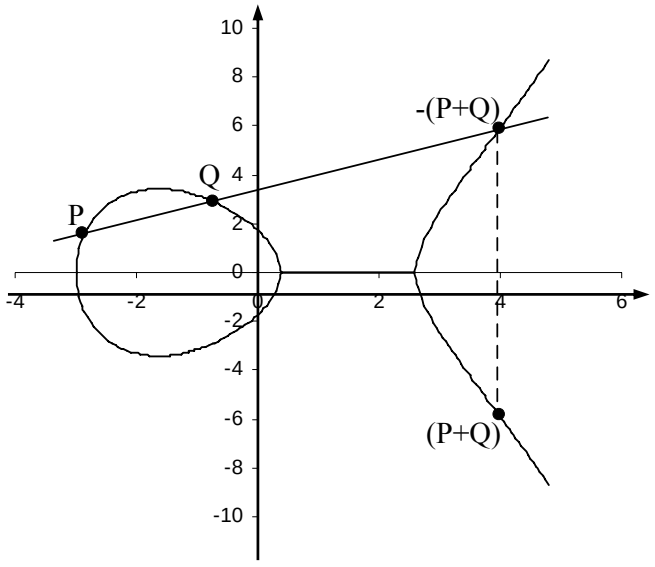
Σχήμα 6.6 Ορισμός αντιθέτου

Παρατηρούμε ότι αν P = (*x*, *y*), τότε –P = (*x*, *–y*). Γεωμετρικά αυτό περιγράφεται ως εξής. Υπολογίζουμε την ευθεία που διέρχεται από το σημείο P και το σημείο **O** (κατακόρυφη). Το τρίτο σημείο της καμπύλης είναι το –P. Το σημείο στο άπειρο είναι το σημείο εκείνο στο οποίο τέμνονται όλες οι παράλληλες με τον άξονα των y.

Επομένως το ουδέτερο στοιχείο στην πρόσθεση σημείων ελλειπτικής καμπύλης είναι το σημείο **O**:

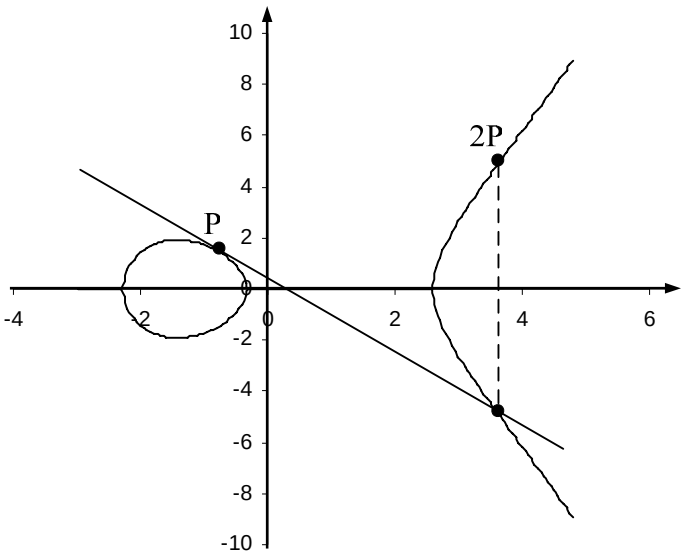
P + **O** = **O** + P = P, και
P + (–P) = **O**.

Έστω τα σημεία P και Q της ελλειπτικής καμπύλης (Σχήμα 6.7). Η ευθεία η οποία διέρχεται από τα P και Q, τέμνει την καμπύλη στο τρίτο σημείο το οποίο είναι το -(P + Q). Το σημείο (P + Q) θα είναι το συμμετρικό του –(P + Q) ως προς τον άξονα x.



Σχήμα 6.7 Πρόσθεση σημείων, P + Q

Στην περίπτωση που P = Q, θεωρούμε ότι τα δύο από τα τρία σημεία που τέμνουν την καμπύλη συμπίπτουν. Η ευθεία που ορίζεται είναι η εφαπτομένη στο σημείο P (Σχήμα 6.8).



Σχήμα 6.8 P + P = 2P

Στη συνέχεια θα περιγράψουμε την πράξη της πρόσθεσης σημείων ελλειπτικής καμπύλης αλγεβρικά. Όπως είδαμε κατά τον γραφικό υπολογισμό, τα δύο σημεία καθώς και το αντίθετο του αθροίσματος αυτών βρίσκονται στην ίδια ευθεία. Έστω τα δύο σημεία $P = (x_1, y_1)$ και $Q = (x_2, y_2)$. Τότε η ευθεία:

$$y = \lambda x + c$$

η οποία διέρχεται από τα σημεία αυτά θα έχει κλίση ίση με:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Αν στην εξίσωση της ελλειπτικής καμπύλης θέσουμε όπου y την εξίσωση ευθείας, οι συντεταγμένες του σημείου $P + Q = (x_3, y_3)$ είναι:

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

Οι παραπάνω σχέσεις προέκυψαν για διαφορετικά σημεία P και Q. Στην περίπτωση όπου $Q = -P = (x_1, -y_1)$, η κλίση γίνεται άπειρη, γεγονός που μας οδηγεί στο σημείο **O**.

Τέλος, στην περίπτωση όπου P = Q, η πρόσθεση αντιστοιχεί με το διπλασιασμό του σημείου P. Η κλίση υπολογίζεται από την παραγώγιση της εξίσωσης της ελλειπτικής καμπύλης και είναι ίση με:

$$\lambda = \frac{3x_1^2 + a}{2y_1},$$

ενώ οι συντεταγμένες ορίζονται από τις σχέσεις που υπολογίσθηκαν για διαφορετικά P και Q.

6.7.2. Οι ελλειπτικές καμπύλες ορισμένες modulo *p*

Η εισαγωγική παρουσίαση των ελλειπτικών καμπυλών στο σώμα των πραγματικών αριθμών, είχε σκοπό τη γραφική απεικόνιση των καμπυλών, και την παρουσίαση των εξισώσεων της πρόσθεσης σημείων της καμπύλης. Οι ελλειπτικές καμπύλες οι οποίες έχουν κρυπτογραφικό ενδιαφέρον είναι ορισμένες στο σώμα $\boldsymbol{Z}_p$, όπου p είναι πρώτος και $p > 3$. Η πράξη της πρόσθεσης είναι επίσης εσωτερική στο $\boldsymbol{Z}_p$, και ορίζεται με τον ίδιο τρόπο. Επίσης μας ενδιαφέρει η ελλειπτική καμπύλη να έχει τρεις διακριτές ρίζες (για $y = 0$), οπότε καταλήγουμε στον ακόλουθο επίσημο ορισμό:

ΟΡΙΣΜΟΣ 6.6 – Η ελλειπτική καμπύλη ορισμένη στο $\boldsymbol{Z}_p$, για κάποιον πρώτο ακέραιο $p > 3$, είναι το σύνολο των στοιχείων $(x, y) \in \boldsymbol{Z}_p \times \boldsymbol{Z}_p$ τα οποία ικανοποιούν την εξίσωση:

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

όπου

$$a, b \in Z_p$$

και

$$4a^3 + 27b^2 \quad 0 \pmod{p}$$

Η πρόσθεση δύο σημείων της ελλειπτικής καμπύλης στο Z_p ορίζεται με τον ίδιο τρόπο όπως και στους πραγματικούς αριθμούς. Έστω δύο σημεία $P = (x_1, y_1)$ και $Q = (x_2, y_2)$, της ελλειπτικής καμπύλης

$$y^2 \equiv x^3 + ax + b \pmod{p}.$$

Το σημείο $P + Q = (x_3, y_3)$ το οποίο είναι επίσης σημείο της καμπύλης, θα έχει συντεταγμένες:

$$x_3 \equiv \lambda^2 - x_1 - x_2 \pmod{p} \quad \text{και}$$
$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod{p}$$

όπου:

$$\lambda \equiv \begin{cases} \dfrac{(y_2 - y_1)}{(x_2 - x_1)} \pmod p, & \text{εάν P} \neq \text{Q} \\ \dfrac{3x_1^2 + a}{2y_1} \pmod p, & \text{εάν P} = \text{Q} \end{cases}$$

Μια άλλη σημαντική ιδιότητα στις ελλειπτικές καμπύλες στο $\boldsymbol{Z}_p$, είναι ότι τα σημεία της ελλειπτικής καμπύλης μαζί με το σημείο **O** ορίζουν κυκλική υποομάδα. Αυτό σημαίνει ότι οποιοδήποτε σημείο ανήκει στην ελλειπτική καμπύλη εκτός του **O,** είναι γεννήτορας αυτής. Δηλαδή, δοθέντος κάποιου σημείου P της καμπύλης, η διαδοχική πρόσθεση του P στον εαυτό του, θα διατρέξει όλα τα σημεία της καμπύλης. Αν η καμπύλη αποτελείται από n σημεία, τότε θα είναι:

$2P = P + P = Q$
$3P = P + 2P = R$
…
$nP = \mathbf{O}$,
$(n+1)P = P$.

ΠΑΡΑΔΕΙΓΜΑ 6.7 – Υπολογισμός σημείων ελλειπτικής καμπύλης.

1. Θεωρούμε την καμπύλη (E): $y^2 = x^3 + 73$ και τα σημεία της $P_1(2, 9)$ και $P_2(3, 10)$. Η ευθεία που διέρχεται από τα σημεία αυτά βρίσκουμε εύκολα ότι είναι η (ε_{12}): $y = x + 7$. Αντικαθιστώντας στην εξίσωση (E) παίρνουμε $(x + 7)^2 = x^3 + 73$, ή $x^3 - x^2 - 14x + 24 = 0$. Η εξίσωση αυτή είναι γνωστό ότι έχει ρίζες τις $x_1 = 2$ και $x_2 = 3$, αφού είναι οι τετμημένες των σημείων που η ευθεία ε_{12} τέμνει την E. Χρησιμοποιώντας τις σχέσεις Vieta μεταξύ των ριζών και συντελεστών ενός πολυωνύμου, έχουμε ότι $x_1 + x_2 + x_3 = 1$, οπότε για την τρίτη ρίζα της εξίσωσης βρίσκουμε, $x_3 = -4$. Τώρα επειδή $y_3 = x_3 + 7$, έχουμε $y_3 = 3$ και $P(-4, 3)$. Επομένως, $P_3 = (-4, -3)$ όπου, $P_3 = P_1 + P_2$. Στη συνέχεια ας υποθέσουμε ότι θέλουμε να προσθέσουμε το P_3 στον εαυτό του. Η κλίση της εφαπτομένης της καμπύλης E στο σημείο P_3 βρίσκεται διαφορίζοντας την εξίσωση (E):

$$2y\mathrm{d}y = 3x^2\mathrm{d}x, \text{ οπότε } \left.\frac{dy}{dx}\right|_{\substack{x=-4 \\ y=-3}} = \left.\frac{3x^2}{2y}\right|_{\substack{x=-4 \\ y=-3}} = -8$$

Σ' αυτήν την περίπτωση, η εφαπτομένη ευθεία έχει εξίσωση, $y = -8(x + 4) - 3$ ή $y = -8x - 35$ και αντικαθιστώντας στην (E) παίρνουμε $(-8x - 35)^2 = x^3 + 73$, ή $x^3 - 64x^2 - 560x - 1152 = 0$. Η εξίσωση αυτή έχει μια διπλή ρίζα, την $x = -4$, που αντιστοιχεί στην τετμημένη του σημείου επαφής. Χρησιμοποιώντας πάλι την αντίστοιχη σχέση Vieta με $x_1 + x_2 + x_3 = 64$ βρίσκουμε ότι η τρίτη ρίζα είναι, $64 - 2(-4) = 72$. Η αντίστοιχη τιμή του y, είναι $y = -8 \cdot 72 - 35$ ή $y = -611$. Αλλάζοντας το πρόσημο για το y προκύπτει

$P_3 + P_3 = (72, 611)$.

2. Στην περίπτωση που θέλουμε να δουλέψουμε με ελλειπτικές καμπύλες modulo n, όπου n ακέραιος μεγαλύτερος του 3, μπορούμε να εφαρμόσουμε παρόμοια τις παραπάνω ιδέες. Για παράδειγμα, ας θεωρήσουμε την καμπύλη

(E): $y^2 \equiv x^3 + 2x + 3 \pmod 5$

Τα σημεία της E είναι τα διατεταγμένα ζεύγη (x, y) mod 5 τα οποία ικανοποιούν την εξίσωση, και το σημείο στο άπειρο. Μπορούμε να τα υπολογίσουμε / απαριθμήσουμε ως εξής. Οι δυνατές περιπτώσεις για το x mod 5 είναι 0, 1, 2, 3 και 4. Αντικαθιστώντας κάθε μια από τις τιμές αυτές στην εξίσωση, βρίσκουμε τις αντίστοιχες τιμές του y που επαληθεύουν την εξίσωση:

$x \equiv 0 \Rightarrow y^2 \equiv 3 \pmod 5 \qquad \Rightarrow \frown$ λύση

$x \equiv 1 \Rightarrow y^2 \equiv 6 \equiv 1 \pmod 5 \quad \Rightarrow y \equiv 1, 4 \pmod 5$

$x \equiv 2 \Rightarrow y^2 \equiv 15 \equiv 0 \pmod 5 \Rightarrow y \equiv 0 \pmod 5$

$x \equiv 3 \Rightarrow y^2 \equiv 36 \equiv 1 \pmod 5 \Rightarrow y \equiv 1, 4 \pmod 5$

$x \equiv 4 \Rightarrow y^2 \equiv 75 \equiv 1 \pmod 5 \Rightarrow y \equiv 0 \pmod 5$

$x \equiv \infty \Rightarrow y \equiv \infty$.

Επομένως τα σημεία της E είναι τα (1, 1), (1, 4), (2, 0), (3, 1), (3, 4), (4, 0) και (∞, ∞).

Η πρόσθεση των σημείων μιας ελλειπτικής καμπύλης, modulo n, γίνεται με τους τύπους που δόθηκαν παραπάνω με την παρατήρηση ότι ένας ρητός αριθμός a/b πρέπει να αντιμετωπιστεί ως ab^{-1}, όπου $b^{-1}b \equiv 1 \pmod n$. Αυτό απαιτεί ότι $\gcd(b, n) = 1$ και είναι το σημείο κλειδί για τη χρήση των ελλειπτικών καμπυλών στην παραγοντοποίηση ακεραίων. Ας προσθέσουμε τα σημεία (1, 4) και (3, 1) της παραπάνω καμπύλης. Η κλίση είναι

$$\lambda \equiv \frac{1-4}{3-1} \equiv 1 \pmod 5.$$

Επομένως,

$x_3 \equiv \lambda^2 - x_1 - x_2 \equiv 1^2 - 1 - 3 \equiv 2 \pmod 5$

$y_3 \equiv \lambda(x_1 - x_3) - y_1 \equiv 1(1 - 2) - 4 \equiv 0 \pmod 5$

που σημαίνει ότι

$(1, 4) + (3, 1) = (2, 0)$.

6.7.3. Οι ελλειπτικές καμπύλες ορισμένες σε $GF(2^n)$

Οι ελλειπτικές καμπύλες μπορούν να ορισθούν στο σώμα $GF(2^n)$. Μαζί με τις ελλειπτικές καμπύλες ορισμένες στο $\boldsymbol{Z}_p$, το Εθνικό Ινστιτούτο Τυποποίησης και τεχνολογίας (NIST), καθόρισε και τις καμπύλες ορισμένες στο $GF(2^n)$. Ο βασικός λόγος επιλογής του σώματος αυτού είναι η αποτελεσματική υλοποίηση των ελλειπτικών καμπυλών στο $GF(2^n)$ στις ψηφιακές τεχνολογίες.

Η εξίσωση της ελλειπτικής καμπύλης ορισμένης στο $GF(2^n)$ είναι η ακόλουθη:

$$y^2 + xy = x^3 + ax^2 + b,$$

όπου $a, b \in GF(2^n)$.

Η πρόσθεση δύο σημείων P = (x_1, y_1)και Q = (x_2, y_2) ορίζεται από τις σχέσεις:

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$$
$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1$$

όπου

$$\lambda = \frac{y_2 + y_1}{x_2 + x_1}.$$

Στην περίπτωση όπου P = Q, η πρόσθεση αντιστοιχεί στο 2P με:

$$x_3 = \lambda^2 + \lambda + a$$
$$y_3 = (\lambda + 1)x_1^2 + x_3$$

όπου

$$\lambda = x_1 + \frac{y_1}{x_1}.$$

Το αντίθετο ενός σημείου P, έχει συντεταγμένες –P = $(x_1, x_1 + y_1)$.

6.7.4. Το πρόβλημα του διακριτού λογάριθμου στις ελλειπτικές καμπύλες

Στις προηγούμενες παραγράφους είδαμε τον τρόπο με τον οποίο γίνεται η πρόσθεση ενός σημείου στον εαυτό του. Δεδομένου ενός σημείου P, μπορούμε να υπολογίσουμε το P + P = 2P, είτε γραφικά με την εφαπτομένη στο P, είτε αλγεβρικά με τις εξισώσεις της πρόσθεσης για P = Q. Προτού παρουσιάσουμε το πρόβλημα του διακριτού λογάριθμου στις ελλειπτικές καμπύλες, θα δείξουμε πως γίνεται ο (βαθμωτός) πολλαπλασιασμός ενός σημείου, δηλαδή τον τρόπο υπολογισμού του nP, για δοσμένο ακέραιο n.

Ο τρόπος υπολογισμού του nP είναι παρόμοιος με τον αλγόριθμο «επαναλαμβανόμενου τετραγωνισμού – και – πολλαπλασιασμού», για τον υπολογισμό ύψωσης ενός αριθμού σε δύναμη.

Ο αλγόριθμος επαναλαμβανόμενου τετραγωνισμού – και – πολλαπλασιασμού είναι μια αποτελεσματική μέθοδος να υψώσουμε έναν αριθμό a σε μια δύναμη n. Στις ελλειπτικές καμπύλες μπορούμε να ονομάσουμε τον αντίστοιχο αλγόριθμο «διπλασιασμού – και – πρόσθεσης», ο οποίος έχει ως εξής.

Έστω ένα σημείο P της ελλειπτικής καμπύλης και έστω ο ακέραιος n. Ζητείται το σημείο που αντιστοιχεί στο nP.

1. Είσοδος: n, P.
2. Έστω Q $\leftarrow$ **O**, $i \leftarrow l - 1$
3. Υπολογίζουμε τη δυαδική αναπαράσταση του n. Έστω $(c_0 c_1 ... c_{l-1})$ η δυαδική λέξη μήκους l bits, όπου
$$n = \sum_{i=0}^{l-1} c_i \cdot 2^i \ .$$
4. Επανέλαβε το βήμα έως ότου $i < 0$:
   Q $\leftarrow$ 2Q
   Αν $c_i = 1$, τότε Q $\leftarrow$ Q + P.
   $i \leftarrow i - 1$
5. Έξοδος: Q.

ΠΑΡΑΔΕΙΓΜΑ 6.8 – Υπολογισμός πολλαπλάσιου σημείου ελλειπτικής καμπύλης. Έστω το σημείο P μιας ελλειπτικής καμπύλης. Ζητείται το 171P.

Θα χρησιμοποιήσουμε τον αλγόριθμο διπλασιασμού – και – πρόσθεσης. Έτσι οι μόνες πράξεις που απαιτούνται για τον υπολογισμό του πολλαπλάσιου, είναι ο διπλασιασμός σημείου και η πρόσθεση του P στο αποτέλεσμα. Η δυαδική αναπαράσταση του ακεραίου 171 είναι $171 = (10101011)_2$. Ξεκινώντας από το σημαντικότερο bit, διπλασιάζοντας στο κάθε βήμα και προσθέτοντας το P όποτε το bit είναι ίσο με **1**, καταλήγουμε στο σημείο:

171 P = 2 (2 (2 (2 (2 (2P) + P)) + P)) + P) + P

Είναι φανερές οι αναλογίες των πράξεων μεταξύ της αριθμητικής κατάλοιπων σε πεπερασμένα σώματα και σε ελλειπτικές καμπύλες. Σε ένα πεπερασμένο σώμα $\boldsymbol{Z}_p$, με γεννήτορα $a \in \boldsymbol{Z}_p$, μπορούμε να αναπαράγουμε όλα τα στοιχεία του συνόλου $\boldsymbol{Z}_p$, υψώνοντας τον γεννήτορα σε εκθέτη: $a^n \pmod p$. Ανάλογα, στις ελλειπτικές καμπύλες, δοθέντος κάποιου σημείου P $\neq$ **O**, μπορούμε να αναπαραγάγουμε όλα τα σημεία της ελλειπτικής καμπύλης, με το βαθμωτό γινόμενο nP $\pmod p$. Στον Πίνακα 6.4 παρουσιάζονται οι αναλογίες μεταξύ αριθμητικής κατάλοιπων σε πεπερασμένα σώματα και σε ελλειπτικές καμπύλες.

Αριθμητική κατάλοιπων σε πεπερασμένα σώματα		Αριθμητική κατάλοιπων σε ελλειπτικές καμπύλες
πολλαπλασιασμός	↔	πρόσθεση
ύψωση σε εκθέτη	↔	βαθμωτό γινόμενο

Πίνακας 6.4 Αναλογίες μεταξύ πεπερασμένων σωμάτων και ελλειπτικών καμπυλών

Με βάση την παραπάνω αναλογία μπορούμε πλέον να ορίσουμε το πρόβλημα του διακριτού λογάριθμου στις ελλειπτικές καμπύλες.

ΟΡΙΣΜΟΣ 6.7 – Έστω μια ελλειπτική καμπύλη ορισμένη στο $\boldsymbol{Z}_p$. Έστω ένα σημείο P της καμπύλης και ένα σημείο Q το οποίο αποτελεί βαθμωτό γινόμενο του P. Το πρόβλημα του διακριτού λογάριθμου στην ελλειπτική καμπύλη είναι ο καθορισμός της λύσης n, για την οποία είναι:

$n\mathrm{P} = \mathrm{Q}$.

6.7.5. Ασφάλεια των ελλειπτικών καμπυλών

Έχει δειχθεί ότι η πολυπλοκότητα των μεθόδων που επιχειρούν να λύσουν το πρόβλημα του διακριτού λογάριθμου στις ελλειπτικές καμπύλες είναι της μορφής n^a, $a > 0$. Είναι δηλαδή εκθετικά πιο αργοί από την (λογαριθμική) πολυπλοκότητα του υπολογισμού βαθμωτών γινομένων του P.

Ωστόσο, υπάρχει μια κατηγορία ελλειπτικών καμπυλών, οι υπεριδιάζουσες (supersingular) ελλειπτικές καμπύλες οι οποίες δεν θεωρούνται ασφαλείς, διότι υποπίπτουν σε επίθεση η οποία εκμεταλλεύεται έναν συγκεκριμένο ισομορφισμό μεταξύ των ελλειπτικών καμπυλών και των πεπερασμένων σωμάτων. Αν και οι συγκεκριμένες ελλειπτικές καμπύλες προτιμούνται λόγω της αποτελεσματικής σε ταχύτητα υλοποίησης των πράξεων, δεν συνιστώνται.

Ένα άλλο κριτήριο ασφάλειας των ελλειπτικών καμπυλών είναι το πλήθος των σημείων μιας ελλειπτικής καμπύλης. Όσο μεγαλύτερος είναι ο αριθμός των σημείων μιας καμπύλης, τόσο μεγαλύτερη θα είναι και η εξαντλητική αναζήτηση. Γενικά, ο υπολογισμός σημείων μιας ελλειπτικής καμπύλης είναι δύσκολος. Ο Hasse διατύπωσε ένα θεώρημα το οποίο θέτει τα όρια του πλήθους των στοιχείων της ελλειπτικής καμπύλης. Σύμφωνα λοιπόν με τον Hasse, μια καμπύλη ορισμένη στο $\boldsymbol{Z}_p$, αναμένεται να έχει σημεία μεταξύ των ορίων:

$$p + 1 - 2\sqrt{p} \le |E| \le p + 1 + 2\sqrt{p}\,,$$

όπου $|E|$ το πλήθος των σημείων της ελλειπτικής καμπύλης.

Οι Lenstra και Verheul εκτίμησαν ότι προκειμένου μια ελλειπτική καμπύλη να είναι ασφαλής έως το έτος 2020, η τάξη μεγέθους του p είναι 2^{160}, στην περίπτωση του $\boldsymbol{Z}_p$, και $n \approx 160$, στην περίπτωση του $GF(2^n)$. Συγκριτικά, για να έχουμε τον ίδιο βαθμό ασφάλειας στο πεπερασμένο σώμα $\boldsymbol{Z}_p$ με γεννήτορα $a \in \boldsymbol{Z}_p$, και αντίστοιχη πράξη το γινόμενο, η τάξη μεγέθους του p θα πρέπει να είναι 2^{1880}.

6.7.6. Κρυπτογραφία σε ελλειπτικές καμπύλες: ElGamal

Όπως αναφέραμε στην εισαγωγή των ελλειπτικών καμπυλών, οι ελλειπτικές καμπύλες δεν αποτελούν ένα νέο κρυπτοσύστημα, αλλά διατίθενται ως εργαλεία για την υλοποίηση υπαρχόντων κρυπτοσυστημάτων. Ένα από τα πιο απλά κρυπτοσυστήματα ελλειπτικών καμπυλών είναι το κρυπτοσύστημα ElGamal το οποίο θα παρουσιάσουμε στη συνέχεια, και θα χρησιμοποιήσουμε το κρυπτοσύστημα αυτό ως βάση αντιστοίχισης των εννοιών ενός κρυπτοσυστήματος στο σώμα των ελλειπτικών καμπυλών.

Το σύνολο των απλών κειμένων καθώς και το σύνολο των κρυπτοκειμένων αποτελείται από τα σημεία μιας ελλειπτικής καμπύλης. Υπάρχουν αποτελεσματικοί αλγόριθμοι οι οποίοι αντιστοιχίζουν απλό κείμενο σε σημεία ελλειπτικής καμπύλης. Έτσι, ένα απλό κείμενο εκφράζεται με τις συντεταγμένες ενός σημείου:

$$P_m = (x_m, y_m).$$

Για μια ακόμη φορά στο μοντέλο επικοινωνίας θεωρούμε την Αλίκη η οποία επιθυμεί να στείλει εμπιστευτικά ένα μήνυμα στον Βύρωνα. Όπως όλα τα συστήματα ασύμμετρης κρυπτογραφίας, απαιτείται μια αναφορική ποσότητα από την οποία θα προκύψουν το δημόσιο και ιδιωτικό κλειδί. Στις ελλειπτικές καμπύλες, η ποσότητα αυτή θα είναι ένα σημείο της ελλειπτικής καμπύλης. Έστω $G = (x_g, y_g)$ το σημείο αυτό. Ο Βύρων επιλέγει έναν ακέραιο n_b, ο οποίος αποτελεί το ιδιωτικό του κλειδί. Το δημόσιο κλειδί είναι το $\{P_b, G, a, b\}$, όπου:

$$P_b = n_b G.$$

Η Αλίκη γνωρίζοντας το δημόσιο κλειδί του Βύρωνα, επιλέγει έναν ακέραιο k, και κρυπτογραφεί το μήνυμα P_m σύμφωνα με την κρυπτογραφική πράξη:

$$C_m = (kG, P_m + kP_b).$$

Παρατηρούμε από την παραπάνω πράξη ότι το κρυπτοκείμενο αποτελείται από δύο σημεία. Η αποκρυπτογράφηση εκτελείται από τον Βύρωνα ως εξής. Για το ζεύγος σημείων που ορίζουν το κρυπτοκείμενο, πολλαπλασιάζει το πρώτο σημείο με το ιδιωτικό του κλειδί, και το αποτέλεσμα που προκύπτει αφαιρείται από το δεύτερο σημείο:

$$d_k(C_m) = (P_m + kP_b) - (n_b(kG)) = P_m + kn_bG - kn_bG = P_m$$

ΠΑΡΑΔΕΙΓΜΑ 6.9 – Κρυπτοσύστημα ElGamal ορισμένο σε ελλειπτική καμπύλη.

Για παράδειγμα, θεωρούμε ένα κρυπτοσύστημα ElGamal επί της ελλειπτικής καμπύλης (E): $y^2 \equiv x^3 + 19 \pmod{71}$. Ο Βύρων δημοσιοποιεί τον $p = 71$ και ένα σημείο $G = (25, 33)$ της καμπύλης, καθώς και το δημόσιο κλειδί $P_b = n_bG = (33, 39)$ για το ιδιωτικό του κλειδί $n_b = 43$. Για να κρυπτογραφήσει το μήνυμα $P_m = (x_m, y_m) = (22, 44)$, η Αλίκη επιλέγει τυχαία τον μυστικό της ακέραιο ο οποίος ας υπο-

θέσουμε ότι είναι ο $k = 29$. Στη συνέχεια βρίσκει δύο σημεία $R = kG = (33, 32)$ και $Q = kP_b = (25, 38)$. Το μήνυμα P_m κρυπτογραφείται χρησιμοποιώντας τις συντεταγμένες του σημείου Q ώστε $c_x \equiv x_m \cdot 25 \equiv 53 \pmod{71}$ και $c_y \equiv y_m \cdot 38 \equiv 39 \pmod{71}$. Το κρυπτοκείμενο $c = (R, 53, 39)$ αποστέλλεται στον Βύρωνα. Ο Βύρων ανακατασκευάζει το σημείο Q, χρησιμοποιώντας τον μυστικό του ακέραιο n_b ως $Q = n_bR = (25, 38)$, υπολογίζει $25^{-1} \equiv 54 \pmod{71}$ και $38^{-1} \equiv 43 \pmod{71}$. Προφανώς είναι $x_m \equiv 53 \cdot 54 \equiv 2862 \equiv 22 \pmod{71}$ και $y_m \equiv 39 \cdot 43 \equiv 1677 \equiv 44 \pmod{71}$.

Είναι φανερό ότι η ασφάλεια του κρυπτοσυστήματος ElGamal βασίζεται στο πρόβλημα του διακριτού λογάριθμου, όπως αυτός ορίζεται στις ελλειπτικές καμπύλες. Ο αντίπαλος έχει γνώση των $\{ P_b, G, a, b \}$, και από αυτά καλείται να ανακαλύψει το n_b που συνδέει τα P_b και G.

Όροι-κλειδιά του κεφαλαίου

- μυστική πόρτα μονόδρομης συνάρτησης
- επίθεση πιθανού μηνύματος
- γνησίως αύξουσα και υπεραύξουσα ακολουθία
- RSA και παραγοντοποίηση σύνθετου ακεραίου
- El Gamal και διακριτός λογάριθμος
- ιδιάζουσα ελλειπτική καμπύλη

6.8. Ασκήσεις

1. Δίνεται το knapsack (3, 5, 7, 19, 22, 29). Ελέγξτε αν υπάρχει λύση για τα παρακάτω αθροίσματα:
   44 42 60 37 35
2. Δίνεται η υπεραύξουσα ακολουθία (3, 6, 11, 22, 43, 87). Μετατρέψτε την σε δύσκολο knapsack με το κλειδί 7 mod 13.
3. Δίνεται το δύσκολο knapsack (7, 14, 49, 82, 88, 98), το οποίο δημιουργήθηκε με το κλειδί 7 mod 101. Υπολογίστε την αρχική υπεραύξουσα ακολουθία.
4. Κρυπτογραφήστε το απλό κείμενο:
   $\mathbf{P} = (100110\ 110011)_2$
   με το δύσκολο knapsack της άσκησης 3.
5. Κρυπτογραφήστε το απλό κείμενο:
   $\mathbf{P} = (110100\ 010111)_2$
   με το εύκολο knapsack (την υπεραύξουσα ακολουθία) της άσκησης 3.
6. Αποκρυπτογραφείστε το κρυπτοκείμενο
   $\mathbf{C} = (236)$
   το οποίο δημιουργήθηκε με το knapsack της άσκησης 3.
7. Δίνεται το δημόσιο κλειδί κρυπτοσυστήματος RSA:
   $k_e = 7$, $n = 352$.

Από την παραπάνω πληροφορία ανακαλύψτε το ιδιωτικό κλειδί.

8. Κατασκευάστε κρυπτοσύστημα RSA το οποίο να μπορεί να κρυπτογραφεί μηνύματα των 12 bits.
9. Σε ένα κρυπτοσύστημα RSA, οι πρώτοι αριθμοί p και q έχουν μέγεθος ίσο με 80 bits. Έστω ότι μια κρυπταναλυτική επίθεση παραγοντοποίησης του $n = pq$ μπορεί να πραγματοποιηθεί με επιτυχία σε 24 ώρες. Αν διπλασιασθούν τα μεγέθη των πρώτων αριθμών, πόσος χρόνος απαιτείται για να επιτύχει η επίθεση; Θεωρείστε ότι η υπολογιστική ισχύς είναι η ίδια και στις δύο επιθέσεις.
10. Η Αλίκη έχει στην κατοχή της το δημόσιο κλειδί του Βύρωνα, που καθορίζει κρυπτοσύστημα RSA με n μεγέθους 4096 bits. Η Αλίκη αποφασίζει να στείλει μήνυμα στον Βύρωνα, κρυπτογραφώντας όμως το κάθε γράμμα του μηνύματος χωριστά, αντί να χωρίσει το μήνυμα σε τμήματα των 4096 bits. Είναι ασφαλές το σενάριο αυτό;
11. (Αποτυχία πρωτοκόλλου του Stinson) Δείξτε πως μπορεί ο αντίπαλος να ανακαλύψει το απλό κείμενο x, αν χρησιμοποιηθούν τρία διαφορετικά moduli με ίδιο δημόσιο κλειδί, δηλαδή $y_1 = x^3 \bmod n_1$, $y_2 = x^3 \bmod n_2$ και $y_3 = x^3 \bmod n_3$, όταν τα n_1, n_2, n_3 δεν έχουν κοινούς παράγοντες μεταξύ τους (και χωρίς να παραγοντοποιήσετε τα moduli αυτά).
12. Εξετάστε ποιες από τις παρακάτω ελλειπτικές καμπύλες είναι ιδιάζουσες:
    $y^2 = x^3 + x^2 + 5 \mod 11$, $y^2 = x^3 + 2x^2 + 3 \mod 11$
    $y^2 = x^3 + 3x^2 + 8 \mod 17$ $y^2 = x^3 + x^2 + 6 \mod 17$
13. Δίνονται, η ελλειπτική καμπύλη
    $y^2 = x^3 + x^2 + 6 \mod 11$
    και τα σημεία P = (2, 5) και Q = (3, 7). Υπολογίστε τα σημεία P + Q, 2P, 2P + 2Q.