Διάφορες ὄψεις τῆς Κρυπτογραφίας δημοσίου κλειδιοῦ

Καθηγητὴς Ν.Γ. Τζανάκης

Τελευταία ἐνημέρωση 11/1/2008

Στὰ παρακάτω, ἡ Ἀνθὴ (**A**) καὶ ὁ Βασίλης (**B**) ἐπιδιώκουν νὰ ἐπικοινωνήσουν ἀπορρήτως, ἐνῶ ὁ Γάϊος (**Γ**) θέλει νὰ μάθει τὸ περιεχόμενο τῶν μηνυμάτων τους. Ὁ Γάϊος θεωροῦμε ὅτι μπορεῖ νὰ ὑποκλέπτει ὁποιοδήποτε μήνυμα, διότι οἱ δίαυλοι ἐπικοινωνίας εἶναι, πρακτικῶς, ἀνασφαλεῖς. Τὸ θέμα εἶναι νὰ μὴ μπορεῖ νὰ τὸ ἀποκρυπτογραφήσει.

Συμβολισμός. Κάποιες φορὲς θὰ κάνομε χρήση τοῦ παρακάτω συμβολισμοῦ, ὁ ὁποῖος δὲν εἶναι καθιερωμένος, γι' αὐτὸ καὶ τὸν σημειώνομε ἐδῶ: Γιὰ ἀκεραίους x, n, $n > 1$, μὲ $[x]_n$ συμβολίζομε τὸ ὑπόλοιπο τῆς εὐκλειδειας διαίρεσης τοῦ x διὰ n. Ἄρα, (α′) $[x]_n \equiv x \pmod{n}$, καὶ (β′) $[x]_n \in \{0, 1, \ldots, n-1\}$.

1 Ἀνταλλαγὴ κλειδιῶν

Ἡ μέθοδος Κρυπτογραφίας DES καὶ οἱ μεταγενέστερες βελτιώσεις της, θὰ ἦταν «ἀπολύτως ἀσφαλεῖς» ἂν μποροῦσαν οἱ οἱ ἐπικοινωνοῦντες νὰ ἀνταλλάσουν τὰ διάφορα κλειδιά, ποὺ ὑπεισέρχονται στὴν κρυπτογράφηση μὲ «ἀπόλυτη ἀσφάλεια». Αὐτὸ ἐπιτυγχάνεται μὲ τὴ βοήθεια τῆς *Κρυπτογραφίας δημοσίου κλειδιοῦ*. Δηλαδή, στὴν πράξη, τὸ κύριο περιεχόμενο τοῦ μηνύματος μπορεῖ νὰ κρυπτογραφηθεῖ μὲ ἕνα σύστημα ὅπως τὸ DES, καὶ τὰ κλειδιά, ποὺ ὑπεισέρχονται σὲ μία τέτοια κρυπτογράφηση, νὰ κρυπτογραφηθοῦν μὲ ἕνα κρυπτοσύστημα δημοσίου κλειδιοῦ.

1.1 Πρωτόκολλο Diffie-Hellman ἀνταλλαγῆς κλειδιῶν

Ἡ Α καὶ ὁ Β συμφωνοῦν στὴ χρήση ἑνὸς μεγάλου πρώτου p (ἂς ποῦμε, τῆς τάξεως τῶν 1024 bits), καθὼς καὶ σὲ ἕνα γεννήτορα g τῆς ὁμάδας $\mathbb{F}_p^*$. Ὑποτίθεται ὅτι τὰ στοιχεῖα αὐτῆς τῆς ὁμάδας ἐκπροσωποῦνται ἀπὸ τοὺς

ἀκεραίους $1, 2, \ldots, p-1$, ὁπότε, ὕστερα ἀπὸ κάθε ἀριθμητικὴ πράξη γίνεται ἀναγωγὴ $\bmod p$. Τέλος, τὰ p καὶ g, πρακτικῶς, θεωροῦνται δημόσια.

1. Ἡ Α ἐπιλέγει τυχαῖα ἕνα μεγάλο $a \in \mathbb{N}$ καὶ ὑπολογίζει τὸ $m_A = g^a$, τὸ ὁποῖο καὶ στέλνει στὸν Β.

2. Ὁ Β ἐπιλέγει τυχαῖα ἕνα μεγάλο $b \in \mathbb{N}$ καὶ ὑπολογίζει τὸ $m_B = g^b$, τὸ ὁποῖο καὶ στέλνει στὴν Α.

3. Ἡ Α ἔλαβε τὸ m_B καὶ ξέρει (εἶναι δικό της) τὸ a, ἄρα μπορεῖ νὰ ὑπολογίσει τὸ $m_B^a \in \mathbb{F}_p^*$.

4. Ὁ Β ἔλαβε τὸ m_A καὶ ξέρει (εἶναι δικό του) τὸ b, ἄρα μπορεῖ νὰ ὑπολογίσει τὸ $m_A^b \in \mathbb{F}_p^*$.

5. Τὸ κλειδί, στὸ ὁποῖο συμφώνησε ἡ Α καὶ ὁ Β εἶναι ἡ κοινὴ τιμή, ἔστω $k \in \mathbb{F}_p^*$ τῶν m_B^a καὶ m_A^b.

Πράγματι, $m_B^a = (g^b)^a = g^{ba}$ καί, ἀνάλογα, $m_A^b = g^{ba}$, ἄρα, ὄντως ἡ Α καὶ ὁ Β θὰ ὑπολογίσουν τὴν ἴδια τιμὴ k.

Ὁ Γ, προκειμένου νὰ μάθει τὴν τιμὴ τοῦ k ἔχει νὰ λύσει τὸ ἑξῆς :

Πρόβλημα Diffie-Hellman 1.1.1. *Ἂν εἶναι γνωστὸς ὁ πρῶτος p, ἕνας γεννήτορας g τῆς ὁμάδας $\mathbb{F}_p^*$ καὶ τὰ στοιχεῖα g^a καὶ g^b τῆς $\mathbb{F}_p^*$, ὑπολόγισε τὸ $g^{ab} \in \mathbb{F}_p^*$.*

Τὸ πρόβλημα αὐτὸ θεωρεῖται ἐξαιρετικὰ δύσκολο ἀπὸ ὑπολογιστικὴ ἄποψη. Σχετίζεται ἄμεσα μὲ τὸ ἑξῆς, ἐπίσης ἐξαιρετικὰ δύσκολο, ἀπὸ ὑπολογιστικὴ ἄποψη, πρόβλημα:

Πρόβλημα τοῦ Διακριτοῦ Λογαρίθμου 1.1.2. *Ἂν εἶναι γνωστὸς ὁ πρῶτος p, ἕνας γεννήτορας g τῆς ὁμάδας $\mathbb{F}_p^*$ καὶ τὸ στοιχεῖο g^a, ὑπολόγισε τὸ a.*

Προφανῶς, ἂν μπορεῖ κανεὶς νὰ λύσει το Πρόβλημα 1.1.2, τότε μπορεῖ νὰ λύσει καὶ τὸ Πρόβλημα 1.1.1. Τὸ ἀντίστροφο δὲν εἶναι γνωστὸ ἂν ἰσχύει. Παρὰ τὸ γεγονὸς ὅτι τὸ Πρόβλημα 1.1.1 φαίνεται εὐκολότερο ἀπὸ τὸ Πρόβλημα 1.1.2, ὅλες οἱ ἐνδείξεις συνηγοροῦν ὑπὲρ τῆς ἀπόψεως ὅτι πρόκειται γιὰ ἰσοδύναμης δυσκολίας πρόβλημα! Οἱ καλλίτεροι, μέχρι σήμερα, ἀλγόριθμοι γιὰ τὸν ὑπολογισμὸ τοῦ διακριτοῦ λογαρίθμου εἶναι *ὑποεκθετικοῦ* χρόνου καί, συγκεκριμένα, $\exp(O(\sqrt{\log p \log\log p}))$. Ὑπάρχουν εὔλογα ἐπιχειρήματα, ποὺ ἀκόμη δὲν ἔχουν μετατραπεῖ σὲ αὐστηρὲς ἀποδείξεις, ὅτι ὁ χρόνος αὐτὸς μπορεῖ νὰ βελτιωθεῖ στὸν $\exp(O(\sqrt[3]{\log p \log^2 \log p}))$. Καὶ στὶς

δύο περιπτώσεις, τὸ πρόβλημα εἶναι ἐξαιρετικὰ δύσκολο ἀπὸ ὑπολογιστικὴ ἄποψη.

Ὑπάρχει, παρ' ὅλ' αὐτά, μία, τουλάχιστον, περίπτωση, κατὰ τὴν ὁποία τὸ Πρόβλημα 1.1.2 σχετικὰ εὔκολα: Ὅταν ὁ $p-1$ εἶναι B-ὁμαλός ἀριθμός, δηλαδή, ὅταν στὴν κανονικὴ ἀνάλυσή του σὲ πρώτους παράγοντες ὅλοι οἱ πρῶτοι εἶναι μικρότεροι ἀπὸ κάποιο σχετικὰ πολὺ μικρὸ φρᾶγμα B (π.χ.τῆς τάξεως τοῦ 500) καὶ οἱ ἐκθέτες τους εἶναι, ἐπίσης, μικροί (π.χ. 0 ἢ 1, μὲ ἐξαίρεση τὸν ἐκθέτη τοῦ 2).

Ἔστω πρῶτος p, q ἕνας πρῶτος διαιρέτης τοῦ $p-1$ καὶ q^n ἡ μέγιστη δύναμη τοῦ q, ποὺ διαιρεῖ τὸν $p-1$. Ἔστω g ἕνας γεννήτορας τῆς ὁμάδας $\mathbb{F}_p^*$ καὶ $a \in \mathbb{F}_p^*$. Φυσικά, ἀφοῦ ὁ g εἶναι γεννήτορας, ὑπάρχει $x \in \{0,1,\ldots,p-2\}$, τέτοιο ὥστε $g^x = a$, τὸ ὁποῖο, ἐν γένει, εἶναι δύσκολο νὰ ὑπολογισθεῖ. Ἂς ποῦμε ὅτι στὸ σύστημα ἀρίθμησης μὲ βάση q, $x = b_0 + b_1 q + b_2 q^2 + \cdots$, ὅπου, βέβαια, $0 \le b_i < q$ γιὰ $i = 0,1,2,\ldots$. Ὁ παρακάτω ἀλγόριθμος ὑπολογίζει τὰ $b_0, b_1, \ldots, b_{n-1}$.

Ἀλγόριθμος Pohling-Hellman 1.1.3. *b_0 εἶναι ὁ μοναδικὸς ἀκέραιος μέσα ἀπὸ τὸ $\{0,1,\ldots,q-1\}$ γιὰ τὸν ὁποῖον ἰσχύει $g^{b_0(p-1)/q} = a^{(p-1)/q}$.*
Γιὰ κάθε $k = 1,2,\ldots,n-1$ ἡ εὕρεση τοῦ b_k γίνεται ὡς ἑξῆς: Ὑπολογίζομε τὰ $n_k = \sum_{i=0}^{k-1} b_i q^i$ καὶ $a_k = a g^{-n_k}$ καὶ προσδιορίζομε τὸ b_k ὡς τὸν μοναδικὸ ἀκέραιο μέσα ἀπὸ τὸ σύνολο $\{0,1,\ldots,q-1\}$, γιὰ τὸν ὁποῖον ἰσχύει $g^{b_k(p-1)/q} = a_k^{(p-1)/q^{k+1}}$.

Ἡ ἀπόδειξη θὰ δοθεῖ σὲ κάποια διάλεξη.

Μὲ τὴ βοήθεια τοῦ Ἀλγορίθμου 1.1.3, μποροῦμε, συνεπῶς,νὰ ὑπολογίσομε τὸν $x \pmod{q^n}$. Ἔστω, λοιπόν, ὅτι ἡ κανονικὴ ἀνάλυση τοῦ $p-1$ σὲ πρώτους παράγοντες εἶναι

$$p-1 = \prod_{j=1}^{r} q_j^{n_j} .$$

Γιὰ κάθε $j = 1,2,\ldots,r$, ὁ ἀλγόριθμος ὑπολογίζει $a_j \in \{0,1,\ldots,q_j^{n_j}-1\}$, τέτοιο ὥστε $x \equiv a_j \pmod{q_j^{n_j}}$. Μετά, ἀπὸ τὸ *Κινέζικο Θεώρημα*, μποροῦμε νὰ ὑπολογίσομε τὸν x!

Τὸ πλῆθος τῶν ἀπαιτουμένων πράξεων στὴν ὁμάδα $\mathbb{F}_p^*$ γιὰ ὅλη αὐτὴ τὴ διαδικασία (πλὴν τοῦ Κινέζικου Θεωρήματος) εἶναι τῆς τάξεως τοῦ ἀριθμοῦ

$$\sum_{j=1}^{r} n_j (\ln p + \sqrt{q_j}) .$$

Ἂν ὁ $p-1$ ἔχει μικροὺς μόνο πρώτους διαιρέτες, μὲ μικρὸ ἐκθέτη ὁ καθένας, τότε τὸ κόστος ὑπολογισμοῦ εἶναι μικρὸ καὶ ἡ εὕρεση τοῦ x εἶναι ἐφικτή. Γιὰ τέτοιους πρώτους p, τὸ Πρόβλημα 1.1.2 καί, συνεπῶς, καὶ τὸ Πρόβλημα 1.1.1 εἶναι ἐπιλύσιμα ἀπὸ ὑπολογιστικὴ ἄποψη.

Ἄσκηση 1. *Στὸ $\mathbb{F}_p$, μὲ $p = 2161$, ἐφαρμόστε τὸν ἀλγόριθμο Pohling-Hellman γιὰ τὴν ἐπίλυση τῆς $23^x = 1853$. Ἐδῶ, 23 εἶναι ὁ ἐλάχιστος γεννήτορας τῆς $\mathbb{F}_p^*$.*

Στὶς διαλέξεις θὰ παρουσιάσομε ἀκόμη ἕναν ἀλγόριθμο γιὰ τὴν ἐπίλυση τῆς $g^x = c$ στὸ $\mathbb{F}_p$, τὸν λεγόμενο *Ἀλγόριθμο τῶν μικρούτσικων καὶ τῶν γιγάντιων βημάτων* (Baby step-Giant step) τοῦ D. Shanks.

1.2 Πρωτόκολλο Diffie-Hellman ἀνταλλαγῆς κλειδιῶν μὲ ἐλλειπτικὴ καμπύλη

Ἡ Α καὶ ὁ Β συμφωνοῦν στὴ χρήση ἑνὸς μεγάλου πρώτου p, μιᾶς ἐλλειπτικῆς καμπύλης $E : y^2 = x^3 + ax + b$ μὲ $a, b \in \mathbb{Z}$ καὶ ἑνὸς σημείου $P \in E(\mathbb{Q})$ ἄπειρης τάξεως, τοῦ ὁποίου οἱ συντεταγμένες ἔχουν παρονομαστὲς πρώτους πρὸς τὸν p. Πρακτικῶς, εἶναι ἐπιθυμητό, τὸ σημεῖο $\tilde{P} \in \tilde{E}(\mathbb{F}_p)$ νὰ ἔχει τάξη συγκρίσιμη μὲ τὸν p. Ὁ πρῶτος p, ἡ ἐλλειπτικὴ καμπύλη E καὶ τὸ σημεῖο P, πρακτικῶς, θεωροῦνται δημόσια.

1. Ἡ Α ἐπιλέγει τυχαῖα ἕνα μεγάλο $a \in \mathbb{N}$ καὶ ὑπολογίζει τὸ $M_A = a\tilde{P} \in \tilde{E}(\mathbb{F}_p)$, τὸ ὁποῖο καὶ στέλνει στὸν Β.

2. Ὁ Β ἐπιλέγει τυχαῖα ἕνα μεγάλο $b \in \mathbb{N}$ καὶ ὑπολογίζει τὸ $M_B = b\tilde{P} \in \tilde{E}(\mathbb{F}_p)$, τὸ ὁποῖο καὶ στέλνει στὴν Α.

3. Ἡ Α ἔλαβε τὸ M_B καὶ ξέρει (εἶναι δικό της) τὸ a, ἄρα μπορεῖ νὰ ὑπολογίσει τὸ $aM_B \in \tilde{E}(\mathbb{F}_p)$.

4. Ὁ Β ἔλαβε τὸ M_A καὶ ξέρει (εἶναι δικό του) τὸ b, ἄρα μπορεῖ νὰ ὑπολογίσει τὸ $bM_A \in \tilde{E}(\mathbb{F}_p)$.

5. Τὸ κλειδί, στὸ ὁποῖο συμφώνησε ἡ Α καὶ ὁ Β εἶναι ἡ κοινὴ τιμή, ἔστω $K \in \tilde{E}(\mathbb{F}_p)$ τῶν aM_B καὶ bM_A.

Πράγματι, $aM_B = a(b\tilde{P}) = (ab)\tilde{P}$ καί, ἀνάλογα, $bM_A = (ba)\tilde{P}$, ἄρα, ὄντως ἡ Α καὶ ὁ Β θὰ ὑπολογίσουν τὴν ἴδια τιμὴ K. Ἔχοντας τώρα τὸ K, δημιουργοῦν τὸν δυαδικὸ ἀριθμὸ-κλειδί τους, π.χ. μετατρέποντας τὴ x-συντεταγμένη τοῦ K σὲ δυαδικὸ ἀριθμό.

Ὁ Γ, προκειμένου νὰ μάθει τὴν τιμὴ τοῦ K ἔχει νὰ λύσει τὸ ἑξῆς :

Πρόβλημα Diffie-Hellman γιὰ ἐλλειπτικὴ καμπύλη 1.2.1. *Ἂν εἶναι γνωστὸς ὁ πρῶτος p, ἕνας σημεῖο $\tilde{P}$ τῆς ὁμάδας $\tilde{E}(\mathbb{F}_p)$ καὶ τὰ σημεῖα $a\tilde{P}$ καὶ $b\tilde{P}$ τῆς $\tilde{E}(\mathbb{F}_p)$, ὑπολόγισε τὸ $(ab)\tilde{P} \in \tilde{E}(\mathbb{F}_p)$.*

Στενὰ συναρτημένο καί, πιθανότατα, ἰσοδύναμο, ἀπὸ τὴ σκοπιὰ τῆς Θεωρίας Ὑπολογισμοῦ, εἶναι τὸ

Πρόβλημα τοῦ Διακριτοῦ Λογαρίθμου σὲ ἐλλειπτικὴ καμπύλη 1.2.2. *Ἔστω ἐλλειπτικὴ καμπύλη $\tilde{E}$ μὲ συντελεστὲς ἀπὸ τὸ $\mathbb{F}_p^*$ (p πρῶτος) καὶ σημεῖα $\tilde{P}, \tilde{Q} \in \tilde{E}(\mathbb{F}_p)$, γιὰ τὰ ὁποῖα γνωρίζομε ὅτι ὑπάρχει ἀκέραιος n, τέτοιος ὥστε $\tilde{Q} = n\tilde{P}$. Ἂν εἶναι γνωστὰ τὰ $\tilde{P}$ καὶ $\tilde{Q}$, νὰ ὑπολογισθεῖ ὁ n.*

Τὸ πλεονέκτημα τοῦ νὰ χρησιμοποιήσει κανεὶς στὸ πρωτόκολλο ἀνταλλαγῆς κλειδιῶν Diffie-Hellman, τὴν ὁμάδα $\tilde{E}(\mathbb{F}_p)$ ἀντὶ τῆς ὁμάδας $\mathbb{F}_p^*$, ἔγκειται στὸ ὅτι, τὸ πρόβλημα 1.2.2 εἶναι, σύμφωνα μὲ ὅλες τὶς ἐνδείξεις, πολὺ δυσκολώτερο ἀπὸ τὸ πρόβλημα 1.1.2. Ἐνῶ τὸ δεύτερο πρόβλημα, ὅπως ἐπισημάνθηκε στὴν παράγραφο 1.1, εἶναι, ὑποεκθετικῆς ὑπολογιστικῆς δυσκολίας[1], γιὰ τὸ πρῶτο δὲν ἔχει βρεθεῖ μέχρι σήμερα[2] ὑποεκθετικὸς ἀλγόριθμος, ἐκτὸς ἂν ἡ ἐλλειπτικὴ καμπύλη E εἶναι τοῦ εἰδικοῦ τύπου *supersingular*. Φυσικά, μπορεῖ νὰ χρησιμοποιήσει κανεὶς τὸν γενικὸ ἀλγόριθμο γιὰ τὸ ἑξῆς

Γενικὸ Πρόβλημα Διακριτοῦ Λογαρίθμου 1.2.3. *Ἔστω $(G, \cdot)$ πεπερασμένη ὁμάδα καὶ $g \in G$*[3] *Ἂν $a \in \langle g \rangle$, νὰ ὑπολογισθεῖ ἀκέραιος x, τέτοιος ὥστε $g^x = a$.*

Οἱ γνωστοὶ ἀλγόριθμοι, ὅμως, γιὰ τὴν ἐπίλυση αὐτοῦ τοῦ προβλήματος εἶναι ἐκθετικοῦ χρόνου, δηλαδή, χρόνου $\exp(O(\log p))$, στὴν περίπτωση ποὺ ἡ τάξη τῆς ὁμάδος διαιρεῖται ἀπὸ ἕνα πρῶτο «ὄχι πολὺ μικρότερο» ἀπὸ τὸν p.

2 Κρυπτοσυστήματα δημοσίου κλειδιοῦ

Ὑποτίθεται ὅτι κάθε μήνυμα εἶναι μία ἀκολουθία ἀπὸ ἀράδες (blocks) ἀριθμῶν $\leq N$, γιὰ κάποιον κατάλληλο φυσικὸ ἀριθμὸ N. Γιὰ παράδειγμα, ἂν

[1] Αὐτὸ μέχρι σήμερα (28 Νοεμβρίου 2012)· δὲν ἔχει ἀποκλείσει κανεὶς ὅτι εἶναι ἀκόμη μικρότερης δυσκολίας.

[2] 28 Νοεμβρίου 2012

[3] Σημειῶστε ὅτι δὲν ὑποθέτομε τὴν G κυκλική, ἢ, κι ἂν ἀκόμη εἶναι, δὲν ὑποθέτομε ὅτι ὁ g εἶναι γεννήτοράς της.

χρησιμοποιοῦμε τὸ ἑλληνικὸ ἀλφάβητο μαζὶ μὲ τὸ «κενὸ γράμμα», καὶ ἀριθμήσομε τὸ Α μὲ 01 τὸ Β μὲ 02, . . ., τὸ Ω μὲ 24 καὶ τὸ κενὸ μὲ 25, θὰ μπορούσαμε νὰ κάνομε τὴν ἐπιλογὴ: $N = 25$ καὶ κάθε γράμμα νὰ ἀντιστοιχεῖ σὲ μία ἀράδα. Μία ἄλλη ἐπιλογὴ θὰ ἦταν $N = 2525$ καὶ κάθε ἀράδα νὰ εἶναι ζεῦγος γραμμάτων. Στὴ δεύτερη περίπτωση, τὸ μήνυμα ΣΥΝΑΝΤΗΣΗ ΤΟ ΜΕΣΗΜΕΡΙ εἶναι ἡ ἀκολουθία τῶν ἀριθμῶν 1820,1301,1319,0718,0725,1915,2512,0518,0712,0517, 0925.

2.1 Κρυπτοσύστημα RSA

Πρόκειται γιὰ κρυπτοσύστημα, τοῦ ὁποίου ἡ κρυπτανάλυση *εἰκάζεται* ὅτι εἶναι τόσο δύσκολη, ὅσο καὶ ὁ ὑπολογισμὸς τῆς ἀνάλυσης ἑνὸς ἀκεραίου σὲ πρώτους παράγοντες.

Καθένας, ὁ ὁποῖος ἐπιθυμεῖ νὰ λαμβάνει κρυπτογραφημένα μηνύματα, δημιουργεῖ ἕνα δημόσιο καὶ ἕνα ἰδιωτικὸ κλειδί.

2.1.1 Δημιουργία δημοσίου καὶ ἰδιωτικοῦ κλειδιοῦ

1. Ἐπιλέγονται δύο πολὺ μεγάλοι διαφορετικοὶ πρῶτοι p, q, τῆς αὐτῆς τάξεως μεγέθους, μεγαλύτεροι ἀπὸ τὸν N (βλ. παράγραφο 2) καὶ ὑπολογίζεται ὁ $n = pq$.

2. Ἐπιλέγεται $e \in \mathbb{N}$ τυχαῖο, ἀλλὰ νὰ ἱκανοποιεῖ τοὺς περιορισμοὺς $1 < e < \phi(n)$ καὶ $\gcd(e, \phi(n)) = 1$.

3. Ὑπολογίζεται $d \in \mathbb{N}$, τέτοιο ὥστε $ed \equiv 1 \pmod{\phi(n)}$.

4. **Δημόσιο κλειδὶ** εἶναι τὸ (n, e) καὶ **ἰδιωτικὸ κλειδὶ** τὸ d.

2.1.2 Κρυπτογράφηση

Ἡ Α, ποὺ ἐπιθυμεῖ νὰ στείλει στὸν Β κρυπτογραφημένο μήνυμα, κάνει τὰ ἑξῆς :

1. Μετατρέπει τὸ μήνυμά της σὲ ἀκολουθία ἀριθμῶν m, μὲ $m \leq N$.

2. Πληροφορεῖται τὸ δημόσιο κλειδὶ (n, e) τοῦ Β.

3. Γιὰ κάθε m τοῦ μηνύματός της ὑπολογίζει τὸ $c \equiv m^e \pmod{n}$.

4. Στέλνει ἕνα πρὸς ἕνα ὅλα τὰ c στὸν Β.

2.1.3 Ἀποκρυπτογράφηση

Ὁ Β χρησιμοποιεῖ τὸ μυστικὸ κλειδί του d, καὶ γιὰ κάθε c, τὸ ὁποῖο λαμβάνει ὑπολογίζει τὸ $c^d \pmod{n}$, βρίσκοντας τὸ m, ἀπὸ τὸ ὁποῖο προῆλθε τὸ c.

2.1.4 Θέματα ἀσφαλείας

1. Ὁ Γ, ποὺ ὑποκλέπτει τὸ κρυπτογραφημένο μήνυμα c καὶ θέλει νὰ μάθει τὸ περιεχόμενο τοῦ m, βρίσκεται ἀντιμέτωπος μὲ τὸ ἑξῆς πρόβλημα:
Πρόβλημα RSA. *Δεδομένου τοῦ σύνθετου ἀριθμοῦ n, τοῦ ἀκεραίου e, ὁ ὁποῖος εἶναι πρῶτος πρὸς τὸν n, καὶ τοῦ ἀκεραίου c, νὰ λυθεῖ ἡ ἰσοτιμία $x^e \equiv c \pmod{n}$.*
Ὁ μόνος γνωστὸς τρόπος μέχρι σήμερα γιὰ νὰ λύσει κανεὶς μιὰ τέτοια ἰσοτιμία, εἶναι νὰ παραγοντοποιήσει τὸ n καὶ νὰ ἐπιλύσει ὕστερα τὶς ἰσοτιμίες $\bmod p$ γιὰ ὅλους τοὺς πρώτους διαιρέτες p τοῦ n. Ἄρα, ἂν μποροῦμε νὰ παραγοντοποιοῦμε σύνθετους n, ποὺ ἔχουν δύο τουλάχιστον πολὺ μεγάλους πρώτους διαιρέτες, τότε μποροῦμε νὰ λύσομε τὸ πρόβλημα RSA. Ἰσχύει τὸ ἀντίστροφο; Δὲν εἶναι γνωστὸ μέχρι σήμερα[4], ἀλλὰ ἔχει ἀποδειχθεῖ ὅτι, ἂν ναί, τότε καὶ τὰ δύο προβλήματα –τῆς παραγοντοποίησης ἀκεραίου καὶ τὸ RSA– εἶναι εὔκολα (πολυωνυμικοῦ χρόνου)! Ἡ μέχρι τώρα ἐμπειρία δὲν εὐνοεῖ ἕνα τέτοιο σενάριο. Εἶναι εὐκολώτερο τὸ πρόβλημα RSA ἀπὸ τὸ πρόβλημα τῆς παραγοντοποίησης; Καὶ πάλι, δὲν ἔχομε σοβαρὲς ἐνδείξεις γιὰ κάτι τέτοιο. Συνεπῶς, μποροῦμε νὰ θεωροῦμε τὸ πρόβλημα RSA ὡς ἕνα πρακτικῶς ἄλυτο πρόβλημα ὅταν $n = pq$, ὅπου οἱ διαφορετικοὶ πρῶτοι p, q εἶναι πολὺ μεγάλοι, ἂς ποῦμε, τῆς τάξεως τοῦ 2^{512}.

2. Ἂν ὁ Β λάβει ἕνα κρυπτογραφημένο μήνυμα ἀπὸ τὸν Γ καὶ μετὰ ὁ Γ ζητήσει ἀπὸ τὸν Β νὰ τοῦ ἀποκρυπτογραφήσει αὐτὸ τὸ μήνυμα[5], ὁ Β πρέπει νὰ ἀρνηθεῖ. Πράγματι, δέστε τὸ ἑξῆς σενάριο: Ἡ Α κρυπτογραφεῖ κάποιο μήνυμα m μὲ τὸ δημόσιο κλειδὶ (n, e) τοῦ Β. Τὸ κρυπτογραφημένο μήνυμα, ἔστω c, τὸ λαμβάνει ὁ Β, ἀλλὰ τὸ ὑποκλέπτει καὶ ὁ Γ, ὁ ὁποῖος θὰ ἤθελε νὰ μάθει τὸ m. Ἐπιλέγει (ὁ Γ) ἕνα αὐθαίρετο x πρῶτο πρὸς τὸν n, ὑπολογίζει $c' = cx^e$ καὶ στέλνει τὸ c' στὸν Β. Ὕστερα ἰσχυρίζεται στὸν Β ὅτι τὸ c' εἶναι ἡ κρυπτογράφηση κάποιου μηνύματός του, τὸ ὁποῖο ξέχασε, καὶ τοῦ ζητάει νὰ τοῦ τὸ ἀποκρυπτογραφήσει. Ὁ Β πέφτει στὴν παγίδα καὶ τοῦ τὸ ἀποκρυπτογραφεῖ, δηλαδή, ὑπολογίζει τὸ c'^d, ὅπου d εἶναι τὸ ἰδιωτικὸ

[4] 28 Νοεμβρίου 2012

[5] Μὲ τὴν αἰτιολογία, π.χ. ὅτι τὸ ξέχασε· θυμηθεῖτε ὅτι, ἂν ὁ Γ κρυπτογραφήσει ἕνα μήνυμα, τὸ στείλει στὸν Β καὶ μετὰ τὸ ξεχάσει, εἶναι ἀδύνατον νὰ τὸ ἀνακτήσει δίχως τὸ ἰδιωτικὸ κλειδὶ τοῦ Β.

κλειδί του (τοῦ Β), καὶ τὸ γνωστοποιεῖ στὸν Γ.

Ἄσκηση 2. *Γιατὶ τώρα ὁ Γ εἶναι πολὺ εὔκολο νὰ μάθει τὸ m;*

3. Ἕνας διαχειριστὴς δικτύου μιᾶς ἑταιρείας διανέμει στὰ μέλη $1, 2, \ldots, k$ τῆς ἑταιρείας κλειδιὰ (n, e_i) (δημόσια) καὶ d_i (ἰδιωτικά), ὅπου τὸ n εἶναι κοινὸ γιὰ ὅλα τὰ μέλη $i = 1, \ldots, k$. Φυσικά, γιὰ κάθε i, τὸ κλειδὶ d_i εἶναι γνωστὸ μόνο στὸ μέλος i καὶ στὸν διαχειριστή, ὁ ὁποῖος ὑποθέτομε ὅτι εἶναι ἀπολύτως τίμιος καὶ ἐχέμυθος. Παρ' ὅλ' αὐτά, ἡ ἰδέα νὰ χρησιμοποιηθεῖ τὸ ἴδιο n γιὰ ὅλους εἶναι *καταστροφική*: Τὸ κάθε μέλος μπορεῖ νὰ μάθει ὅλα τὰ μηνύματα που στέλνει ὁποιοδήποτε ἄλλο μέλος! Πράγματι, ἀρκεῖ νὰ δείξομε ὅτι καθένα μέλος τῆς ἑταιρείας μπορεῖ, νὰ ἀνακαλύψει τὴν παραγοντοποίηση τοῦ n, ὡς ἑξῆς.
Ἔστω e τὸ δημόσιο καὶ d τὸ ἰδιωτικὸ κλειδί κάποιου μέλους Μ· τὸ n, ὅπως εἴπαμε, εἶναι κοινὸ γιὰ ὅλους. Ὁ Μ ξέρει τὸν ἀριθμὸ $de - 1$ καὶ ξέρει ὅτι αὐτὸς εἶναι διαιρετὸς διὰ $\phi(n) = (p-1)(q-1)$, ἂν καὶ δὲν ξέρει τὸν $\phi(n)$. Ἔστω $de - 1 = 2^s r$, ὅπου ὁ r εἶναι περιττὸς καὶ $s \geq 2$ (γνωστά, φυσικά, στὸν Μ). Ὁ Μ ἀκολουθεῖ τὸν ἑξῆς πιθανοθεωρητικὸ ἀλγόριθμο: Ἐπιλέγει τυχαῖο $x \in \{1, \ldots, n-1\}$ καὶ ὑπολογίζει μκδ(x, n). Ἂν εἶναι μεγαλύτερος τοῦ 1, τότε βρῆκε ἕνα μὴ τετριμμένο παράγοντα τοῦ n, ὁπότε σταματᾶ. Διαφορετικά, προχωρεῖ. Παρακάτω, τὰ $=$ καὶ τὰ $\neq$ ἐννοοῦνται $\bmod n$. Ἀπὸ τὴ σχέση $x^{\phi(n)} = 1$ ἕπεται ἡ $x^{2^s r} = 1$, ἄρα ὑπάρχει ἕνας ἐλάχιστος $t \in \{0, \ldots, s\}$ τέτοιος ὥστε $x^{2^t r} = 1$. Ἂν $t = 0$, ἡ ἐπιλογὴ τοῦ x θεωρεῖται ἀποτυχημένη καὶ ἐπιλέγεται ἄλλο x, μέχρις ὅτου βρεθεῖ x γιὰ τὸ ὁποῖο τὸ ἀντίστοιχο t εἶναι θετικό. Τότε θέτει $y = x^{t-1} r$, ὁπότε $y \neq 1$ καὶ $y^2 = 1$. Ἂν συμβεῖ νὰ εἶναι καὶ $y \neq -1$, τότε ἔχομε τὴν ἑξὴς κατάσταση: $n | (y-1)(y+1)$ καὶ τὸ n δὲν διαιρεῖ οὔτε τὸν $y-1$, οὔτε τὸν $y+1$. Εὔκολα τότε φαίνεται ὅτι ἕνας τουλάχιστον ἀπὸ τοὺς μκδ$(n, y-1)$ καὶ μκδ$(n, y+1)$ εἶναι μὴ τετριμμένος παράγοντας τοῦ n. Τὸ ἐρώτημα τώρα εἶναι ἂν ἔχομε μεγάλες πιθανότητες ἐπιτυχοῦς ἐπιλογῆς γιὰ τὸ x. Γιὰ νὰ εἶναι "κακὸ" κάποιο x πρέπει, ἕνα ἀπὸ τὰ δύο νὰ ἰσχύει: Ἢ $x^r = 1$, ἢ τὸ n νὰ διαιρεῖ τὸ $y+1$, ὁπότε (ἂν συμβαίνει τὸ δεύτερο ἐνδεχόμενο) ὑπάρχει κάποιο $j \in \{0, \ldots, s-1\}$ τέτοιο ὥστε $x^{2^j r} = -1$. Θὰ δείξομε στὸ μάθημα ὅτι οἱ μισοί, τὸ πολύ, ἀριθμοὶ $x \in \{1, \ldots, n-1\}$ ἔχουν αὐτὴ τὴν ἰδιότητα (εἶναι "κακοί"). Ἄρα, ὕστερα ἀπὸ m δοκιμές, ἡ πιθανότητα νὰ ἔχομε βρεῖ μόνο κακὰ x εἶναι 2^{-m}, δηλαδή, ἐξαιρετικὰ μικρή.

Ἄσκηση 3. *Αὐτὴ ἡ ἄσκηση δείχνει ότι τὸ νὰ ὑπολογίσει κανεὶς τὸ $\phi(n)$, ὅταν $n = pq$, μὲ p, q διαφορετικοὺς πρώτους, εἶναι τόσο δύσκολο ὅσο καὶ τὸ ν' ἀναλύσει τὸν n στοὺς πρώτους παράγοντές του.*

Ἀποδεῖξτε ὅτι, ἂν ὁ n εἶναι ὅπως παραπάνω καὶ γνωρίζομε τοὺς n καὶ $\phi(n)$, τότε μποροῦμε νὰ ὑπολογίσομε πολὺ εὔκολα τοὺς p, q.

2.2 Κρυπτοσύστημα Rabin

Πρόκειται γιὰ ἀποδείξιμα ἀσφαλὲς κρυπτοσύστημα. Βασίζεται στὸ ἐξαιρετικὰ δύσκολο, ἀπὸ ὑπολογιστικὴ ἄποψη, πρόβλημα τοῦ ὑπολογισμοῦ τετραγωνικῆς ρίζας mod$n$ *ὅταν ὁ n δὲν εἶναι πρῶτος*. Δηλαδή, ἂν γνωρίζομε ὅτι ἡ ἰσοδυναμία $x^2 \equiv a \pmod{n}$ ἔχει λύσεις[6], νὰ τὶς ὑπολογίσομε.

Καθένας, ὁ ὁποῖος ἐπιθυμεῖ νὰ λαμβάνει κρυπτογραφημένα μηνύματα, δημιουργεῖ ἕνα δημόσιο καὶ ἕνα ἰδιωτικὸ κλειδί.

2.2.1 Δημιουργία δημοσίου καὶ ἰδιωτικοῦ κλειδιοῦ

1. Ἐπιλέγονται δύο πολὺ μεγάλοι διαφορετικοὶ πρῶτοι p, q, τῆς αὐτῆς τάξεως μεγέθους, μεγαλύτεροι ἀπὸ τὸν N (βλ. παράγραφο 2) καὶ ὑπολογίζεται ὁ $n = pq$.

2. **Δημόσιο κλειδὶ** εἶναι τὸ n καὶ **ἰδιωτικὸ κλειδὶ** τὸ (p, q).

2.2.2 Κρυπτογράφηση

Ἡ Α, ποὺ ἐπιθυμεῖ νὰ στείλει στὸν Β κρυπτογραφημένο μήνυμα, κάνει τὰ ἑξῆς :

1. Μετατρέπει τὸ μήνυμά της σὲ ἀκολουθία ἀριθμῶν m, μὲ $m \leq N$.

2. Πληροφορεῖται τὸ δημόσιο κλειδὶ n τοῦ Β.

3. Γιὰ κάθε m τοῦ μηνύματός της ὑπολογίζει τὸ $c \equiv m^2 \pmod{n}$.

4. Στέλνει ἕνα πρὸς ἕνα ὅλα τὰ c στὸν Β.

2.2.3 Ἀποκρυπτογράφηση

Ὁ Β, ὁ ὁποῖος γνωρίζει τὴν ἀνάλυση τοῦ n σὲ πρώτους παράγοντες ($n = pq$), ὑπολογίζει, γιὰ κάθε c τῆς Α, τὸ ὁποῖο λαμβάνει, τὶς 4 (ἀκριβῶς) λύσεις της $x^2 \equiv c \pmod{n}$. Μία ἀπὸ αὐτὲς εἶναι ὁ ἀριθμὸς m, τὸν ὁποῖον ἔστειλε ἡ Α.

[6]Πρόκειται γιὰ εὔκολο, ἀπὸ ὑπολογιστικὴ ἄποψη, πρόβλημα, χάρις στὴ *Θεωρία τῶν Τετραγωνικῶν Ὑπολοίπων* καὶ τὸν *Νόμο Τετραγωνικῆς Ἀντιστροφῆς* τοῦ Gauss

Ἡ ἀνάγκη να διακρίνει ὁ Β τὴ μία ἀπὸ τὶς 4 λύσεις, ἀποτελεῖ ἕνα μειονέκτημα αὐτοῦ τοῦ κρυπτοσυστήματος. Ἕνας τρόπος γιὰ νὰ ὑπερπηδηθεῖ αὐτὴ ἡ δυσκολία εἶναι, π.χ. νὰ ἐπαναλαμβάνει ἡ Α, σὲ κάθε m, ποὺ στέλνει στὸν Β, κάποια ἀπὸ τὰ τελευταῖα ψηφία τοῦ m. Ἂν, γιὰ παράδειγμα, τὸ m, ποὺ θέλει νὰ στείλει ἡ Α εἶναι τὸ $m = 67831$, αὐτὴ θὰ στείλει τὸ $c = 67831831^{27}$ ἀντὶ τοῦ $c = 67831^2$. Εἶναι πολὺ ἀπίθανο ὅτι καὶ οἱ ὑπόλοιπες 3 λύσεις τῆς $x^2 \equiv c \pmod{n}$ θὰ ἔχουν ἀνάλογη ἰδιότητα, δηλαδή, νὰ εἶναι τῆς μορφῆς $b_1b_2b_3b_4b_5b_3b_4b_5$.

Ἄσκηση 4. *Σκοπὸς αὐτῆς τῆς ἄσκησης εἶναι νὰ δείξει ὅτι ὁ ὑπολογισμὸς τῆς τετραγωνικῆς ρίζας τοῦ a στὸ $\mathbb{F}_p$, ἐφόσον τὸ a εἶναι τετράγωνο στὸ $\mathbb{F}_p$, εἶναι ἁπλούστατη ὅταν ὁ p εἶναι πρῶτος καὶ $p \equiv 3 \pmod 4$ ἢ $p \equiv 5 \pmod 8$.*
(α΄) Ἂν $p \equiv 3 \pmod 4$, ἀποδεῖξτε ὅτι $(a^{(p+1)/4})^2 \equiv a \pmod p$.
(β΄) Ἂν $p \equiv 5 \pmod 8$, τότε $x^2 \equiv a \pmod p$ γιὰ $x = a^{(p+3)/8}$ ἢ $x = a^{(p+3)/8}2^{(p-1)/4}$.
Θυμηθεῖτε ὅτι, γιὰ τέτοιους p, τὸ 2 δὲν εἶναι τετράγωνο στὸ $\mathbb{F}_p$.
(γ΄) Μένει ἡ περίπτωση $p \equiv 1 \pmod 4$. Στὶς διαλέξεις θὰ παρουσιάσομε μία "μὴ δαπανηρὴ" μέθοδο ὑπολογισμοῦ τετραγωνικῆς ρίζας, ὅταν εἶναι γνωστὸ ἕνα στοιχεῖο $N \in \mathbb{F}_p^*$, τὸ ὁποῖο δὲν εἶναι τετράγωνο. Ἐπειδὴ τὰ μισά, ἀκριβῶς, στοιχεῖα τοῦ $\mathbb{F}_p^*$ εἶναι τετράγωνα, ἔπεται ὅτι ἡ πιθανότητα νὰ ἐπιλέξομε μὴ τετράγωνο ὕστερα ἀπὸ m τυχαῖες ἐπιλογὲς ἀριθμῶν τοῦ $\{1, \ldots, p-1\}$, εἶναι $1 - 2^{-m}$, δηλαδή, ἐξαιρετικὰ μεγάλη.

2.3 Κρυπτοσύστημα El Gamal

Πρόκειται γιὰ κρυπτοσύστημα, τοῦ ὁποίου ἡ ἀσφάλεια βασίζεται στὸ ἀνέφικτὸ τῆς πρακτικῆς ἐπιλύσεως τοῦ προβλήματος τοῦ διακριτοῦ λογαρίθμου (βλ. 1.1.2).

Κάθε μία ἀπὸ τὶς ἐπικοινωνοῦσες ὀντότητες δημιουργεῖ ἕνα δημόσιο καὶ ἕνα ἰδιωτικὸ κλειδί.

2.3.1 Δημιουργία δημοσίου καὶ ἰδιωτικοῦ κλειδιοῦ

1. Ἐπιλέγεται ἕνας πρῶτος ἀριθμὸς p καὶ ἕνας γεννήτορας g τῆς ὁμάδας $\mathbb{F}_p^*$.

2. Ἐπιλέγεται φυσικὸς ἀριθμὸς $a < p - 1$ καὶ ὑπολογίζεται ὁ $b = g^a \in \mathbb{F}_p^*$.

3. **Δημόσιο κλειδὶ** εἶναι τὸ (p, g, b) καὶ **ἰδιωτικὸ κλειδὶ** τὸ a.

[7] Ὑποτίθεται, βέβαια, ὅτι καὶ ὁ «διογκωμένος» m ἐξακολουθεῖ νὰ εἶναι $< n$.

2.3.2 Κρυπτογράφηση

Ἡ Α, ποὺ ἐπιθυμεῖ νὰ στείλει στὸν Β κρυπτογραφημένο μήνυμα, κάνει τὰ ἑξῆς :

1. Μετατρέπει τὸ μήνυμά της σὲ ἀκολουθία ἀριθμῶν m, μὲ $m \leq p-1$.
2. Πληροφορεῖται τὸ δημόσιο κλειδὶ (p, g, b) τοῦ Β.
3. Ἐπιλέγει φυσικὸ ἀριθμὸ $\nu < p-1$.
4. Γιὰ κάθε m τοῦ μηνύματός της ὑπολογίζει τὰ ἑξῆς στοιχεῖα τῆς $\mathbb{F}_p^*$: $c_1 = g^\nu$ καὶ $c_2 = mb^\nu$.
5. Στέλνει ἕνα πρὸς ἕνα ὅλα τὰ (c_1, c_2) στὸν Β.

2.3.3 Ἀποκρυπτογράφηση

Ὁ Β, ὁ ὁποῖος γνωρίζει τὸ a, ὑπολογίζει τὸ m, βάσει τῆς ἰσότητας $m = c_1^{-a} c_2$.

Ἄσκηση 5. *Ἔχοντας ὡς δεδομένο (ἀπολύτως ρεαλιστικό!) ὅτι ὁ ὠτακουστὴς Γ μπορεῖ νὰ ἔχει στὴν κατοχή του πολλὰ ζεύγη (m, c), ὅπου m εἶναι καθαρὸ μήνυμα τῆς Α πρὸς τὸν Β καὶ c ἡ κρυπτογράφηση τοῦ m, ἐξηγεῖστε γιατὶ εἶναι ἐξαιρετικὰ ἀνασφαλὲς νὰ χρησιμοποιεῖ ἡ Α τὴν ἴδια παράμετρο ν σὲ διαφορετικὰ μηνύματά της πρὸς τὸν Β.*

Ἄσκηση 6. *Ἀποδεῖξτε ὅτι, ἂν ὁ ὠτακουστὴς Γ ὑποκλέψει τὴν κρυπτογράφηση (c_1, c_2) τοῦ μηνύματος m, ποὺ ἔστειλε ἡ Α στὸν Β, καὶ θέλει νὰ μάθει τὸ καθαρὸ μήνυμα m, πρέπει νὰ λύσει ἕνα πρόβλημα Diffie-Hellman.*

2.4 Κρυπτοσυστήματα τοῦ γυλιοῦ

Πρόκειται γιὰ κρυπτοσύστημα τῶν ὁποίων ἡ κρυπτανάλυση ἀπαιτεῖ ἐπίλυση ἑνὸς «προβλήματος γυλιοῦ» (knapsack problem)[8], ἤ, σὲ πιὸ λόγια γλῶσσα, «προβλήματος ἀθροίσματος ὑποσυνόλων» (subset sum problem).

Γενικὸ Πρόβλημα τοῦ γυλιοῦ 2.4.1. *Ἂν δοθοῦν οἱ θετικοὶ ἀριθμοὶ $v_0, v_1, \ldots, v_{k-1}, n$, νὰ διαπιστωθεῖ ἂν ὑπάρχουν $\epsilon_0, \epsilon_1, \ldots, \epsilon_{k-1} \in \{0, 1\}$, ἔτσι ὥστε νὰ ἰσχύει ἡ ἰσότητα*

$$\epsilon_0 v_0 + \epsilon_1 v_1 + \cdots + \epsilon_{k-1} v_{k-1} = n \tag{1}$$

[8] Γύλιος ὁ, - κοινῶς γυλιός - εἶδος στρατιωτικοῦ σάκκου πρὸς φύλαξιν τροφίμων ἢ ἄλλων εἰδῶν ἀτομικῆς χρήσεως· «Νέον Λεξικὸν» Δ.Β. Δημητράκου. Στὴν ἀγγλικὴ χρησιμοποιεῖται ὁ ὅρος knapsack.

καὶ ἂν ναί, νὰ ὑπολογισθεῖ, ἔστω καὶ μία τέτοια λύση $(\epsilon_0, \epsilon_1, \ldots, \epsilon_{k-1})$ *τῆς (1).*

Προφανῶς, ἡ λύση τοῦ προβλήματος ἐπιτυγχάνεται ὕστερα ἀπὸ 2^k δοκιμές, ἀλλὰ μιὰ τέτοια λύση «ἐκθετικοῦ χρόνου», εἶναι ἡ χειρότερη δυνατή, ἀπὸ ὑπολογιστικὴ ἄποψη. Τὸ πρόβλημα αὐτὸ ἀνήκει στὴν κατηγορία τῶν NP-πλήρων προβλημάτων καί, γι' αὐτό, μέχρι τὸ 1984 ὑπῆρχε ἡ ἄποψη ὅτι, κρυπτοσυστήματα, τῶν ὁποίων ἡ κρυπτανάλυση ἀπαιτεῖ τὴν ἐπίλυση ἑνὸς προβλήματος γυλιοῦ, θὰ ἦταν, πιθανώτατα, ἀποδεδειγμένως ἀσφαλῆ. Ἡ ἄποψη αὐτή, σήμερα, ἔχει ἀνατραπεῖ ὕστερα ἀπὸ τὴ δημοσίευση τῆς ἐργασίας [4]. Παρουσιάζομε ἐδῶ αὐτὰ τὰ κρυπτοσυστήματα γιὰ νὰ καταδειχθεῖ ἡ ποικιλία τῶν μαθηματικῶν ἰδεῶν, ποὺ μπορεῖ κανεὶς νὰ ἐφαρμόσει στὴν Κρυπτογραφία καὶ ὡς κίνητρο γιὰ μελέτη συνδυαστικῶν μεθόδων στὴν Κρυπτογραφία (βλ. [2], Κεφάλαιο 5).

Τὸ πρόβλημα 2.4.1 ἀπαντᾶται πολὺ εὔκολα στὴ λεγόμενη *ὑπεραύξουσα περίπτωση*, ὅταν, δηλαδή, $v_j > \sum_{i=0}^{j-1} v_i$ γιὰ κάθε $j = 1, \ldots, k-1$.

Ὁ πολυωνυμικοῦ χρόνου ἀλγόριθμος γιὰ νὰ ἀπαντήσει κανεὶς στὸ πρόβλημα καί, σὲ περίπτωση καταφατικῆς ἀπαντήσεως, νὰ ὑπολογίσει λύση $(\epsilon_0, \epsilon_1, \ldots, \epsilon_{k-1})$, εἶναι ἡ ἑξῆς :

1. $V \leftarrow n$ καὶ $j \leftarrow k$.

2. Ἂν γιὰ ὅλα τὰ $i = 0, 1, \ldots, j-1$ εἶναι $v_i > V$, τὸ πρόβλημα δὲν ἔχει λύση. ΤΕΛΟΣ
   Διαφορετικά, ἔστω i_0 ὁ μέγιστος δείκτης i, τέτοιος ὥστε $v_i \leq V$. Θέσε $\epsilon_{i_0} = 1$ καί $\epsilon_i = 0$ γιὰ $i = i_0 + 1, \ldots, j-1$ ἂν $i_0 < j-1$.
   Πήγαινε στὸ βῆμα 3

3. $V \leftarrow V - v_{i_0}$ καὶ $j \leftarrow i_0$. Πήγαινε στὸ βῆμα 2

Εἶναι εὔκολο νὰ 'δεῖ κανεὶς ὅτι, ἂν τὸ πρόβλημα ἔχει λύση, αὐτὴ εἶναι μοναδική.

Ἐρχόμαστε τώρα στὸ κρυπτοσύστημα Merkle-Hellman. Ὑποτίθεται ὅτι τὰ μηνύματα, ποὺ κρυπτογραφοῦνται εἶναι k-bit ἀράδες. Κάθε μία ἀπὸ τὶς ἐπικοινωνοῦσες ὀντότητες δημιουργεῖ ἕνα δημόσιο καὶ ἕνα ἰδιωτικὸ κλειδί.

2.4.1 Δημιουργία δημοσίου καὶ ἰδιωτικοῦ κλειδιοῦ

1. Ἐπιλέγεται μία ὑπεραύξουσα ἀκολουθία θετικῶν ἀκεραίων $v_0, v_1, \ldots, v_{k-1}$.

2. Ἐπιλέγεται τυχαῖος ἀκέραιος $n > v_0+v_1+\cdots+v_{k-1}$ καὶ θετικὸς ἀκέραιος $a < n$, πρῶτος πρὸς τὸν n.

3. Ὑπολογίζονται $w_0, w_1, \ldots, w_{k-1}$, τέτοια ὥστε, $w_i \equiv av_i \pmod{n}$, $i = 0, \ldots, k-1$.

4. **Δημόσιο κλειδὶ** εἶναι τὸ $(w_0, w_1, \ldots, w_{k-1})$ καὶ **ἰδιωτικὸ κλειδὶ** τὸ $(v_0, v_1, \ldots, v_{k-1}, n, a)$.

2.4.2 Κρυπτογράφηση

Ἡ Α, ποὺ ἐπιθυμεῖ νὰ κρυπτογραφήσει ἕνα μήνυμά της $m = b_{k-1} \ldots b_1 b_0$ (τὰ b_i θὰ συμβολίζουν σὲ αὐτὴ τὴν παράγραφο bits) καὶ νὰ τὸ στείλει στὸν Β, κάνει τὰ ἑξῆς :

1. Πληροφορεῖται τὸ δημόσιο κλειδὶ $(w_0, w_1, \ldots, w_{k-1})$ τοῦ Β.

2. Ὑπολογίζει τὸν ἀριθμὸ $c = \sum_{i=0}^{k-1} b_i w_i$.

3. Στέλνει τὸν c στὸν Β.

2.4.3 Ἀποκρυπτογράφηση

Ὁ Β χρησιμοποιεῖ τὸ μυστικὸ κλειδί του γιὰ νὰ ὑπολογίσει πρῶτα ἕνα d, τέτοιο ὥστε $da \equiv 1 \pmod{n}$ καὶ μετὰ τὸν ἀριθμὸ $N = [dc]_n$. Τέλος, λύνει ἕνα πρόβλημα γυλιοῦ γιὰ τὴν ὑπεραύξουσα ἀκολουθία $v_0, v_1, \ldots, v_{k-1}$ καὶ τὸν ἀριθμὸ N.

Ἀπόδειξη ὅτι ὁ Β θὰ ὑπολογίσει, τελικά, τὸν m. Εἶναι

$$N \equiv dc = \sum_{i=0}^{k-1} b_i dw_i \equiv \sum_{i=0}^{k-1} b_i d(av_i) \equiv \sum_{i=0}^{k-1} b_i (da) v_i \equiv \sum_{i=0}^{k-1} b_i v_i \pmod{n} . \qquad (2)$$

Ἐξ ὁρισμοῦ, $0 \le N < n$, ἐνῶ $\sum_{i=0}^{k-1} b_i v_i < \sum_{i=0}^{k-1} v_i < n$. Ἄρα, τὸ ἀριστερώτερο καὶ τὸ δεξιώτερο μέλος τῆς (2) εἶναι ἀκέραιοι ἀριθμοὶ τοῦ διαστήματος $[0, n-1]$, μεταξύ τους ἰσοδύναμοι mod n. Συνεπῶς, εἶναι ἴσοι. Ἄρα, λύνοντας τὸ πρόβλημα τοῦ γυλιοῦ, ποὺ ἀναφέραμε παραπάνω, ἡ Α θὰ βρεῖ τὰ $b_{k-1}, \ldots, b_1, b_0$, ἀφοῦ τὸ πρόβλημα τοῦ γυλιοῦ στὴν ὑπεραύξουσα περίπτωσή του, ἐφ' ὅσον ἔχει λύση, αὐτὴ εἶναι μοναδική.

Σημειῶστε ὅτι, ἂν ὁ Γ ὑποκλέψει τὸ c, δὲν μπορεῖ νὰ βρεῖ τὰ b_i, διότι θὰ ἔχει νὰ λύσει ἕνα πρόβλημα γυλιοῦ μὲ τὴν ἀκολουθία $w_0, w_1, \ldots, w_{k-1}$, ἡ ὁποῖα δὲν εἶναι ὑπεραύξουσα. Ἄρα, ἀναμενόμενο εἶναι νὰ μὴ μπορέσει νὰ λύσει σὲ ρεαλιστικὸ χρόνο τὸ πρόβλημα. Πράγματι, τὰ $w_0, w_1, \ldots, w_{k-1}$ εἶναι ἀρκετὰ τυχαῖα. Δυστυχῶς, ὅμως, γιὰ τὴν Α (καὶ εὐτυχῶς γιὰ τὸν Γ), τὰ w_i δὲν εἶναι τόσο τυχαῖα. Καὶ αὐτὸ ἐκμεταλλεύθηκε ὁ Shamir[9] γιὰ ν' ἀποδείξει (βλ. [4]) ὅτι ἡ κρυπτανάλυση ἑνὸς τέτοιου κρυπτοσυστήματος μπορεῖ νὰ γίνει σὲ πολυωνυμικὸ χρόνο.

Γιὰ νὰ σώσουν τὴν κατάσταση, οἱ θιασῶτες τῶν κρυπτοσυστημάτων γυλιοῦ πρότειναν τὴν ἑξῆς παραλλαγὴ τοῦ προηγουμένου κρυπτοσυστήματος.

2.4.4 Δημιουργία δημοσίου καὶ ἰδιωτικοῦ κλειδιοῦ

1. Ἐπιλέγεται μία ὑπεραύξουσα ἀκολουθία θετικῶν ἀκεραίων $v_0, v_1, \ldots, v_{k-1}$.
2. Ἐπιλέγεται τυχαῖος ἀκέραιος $n_1 > v_0+v_1+\cdots+v_{k-1}$ καὶ θετικὸς ἀκέραιος $a_1 < n_1$, πρῶτος πρὸς τὸν n_1.
3. Ἐπιλέγεται ἕνας δεύτερος τυχαῖος ἀκέραιος $n_2 > kn_1$ καὶ θετικὸς ἀκέραιος $a_2 < n_2$, πρῶτος πρὸς τὸν n_2.
4. Ὑπολογίζονται τὰ $w_i = [a_1 v_i]_{n_1}$, $i = 0, \ldots, k-1$.
5. Ὑπολογίζονται $u_0, u_1, \ldots, u_{k-1}$, τέτοια ὥστε, $u_i \equiv aw_i \pmod{n_2}$, $i = 0, \ldots, k-1$.
6. **Δημόσιο κλειδὶ** εἶναι τὸ $(u_0, u_1, \ldots, u_{k-1})$ καὶ **ἰδιωτικὸ κλειδὶ** τὸ $(v_0, v_1, \ldots, v_{k-1}, n_1, a_1, n_2, a_2)$.

2.4.5 Κρυπτογράφηση

Ἡ Α, ποὺ ἐπιθυμεῖ νὰ κρυπτογραφήσει ἕνα μήνυμά της $m = b_{k-1} \ldots b_1 b_0$ καὶ νὰ τὸ στείλει στὸν Β, κάνει τὰ ἑξῆς :

1. Πληροφορεῖται τὸ δημόσιο κλειδὶ $(u_0, u_1, \ldots, u_{k-1})$ τοῦ Β.
2. Ὑπολογίζει τὸν ἀριθμὸ $c = \sum_{i=0}^{k-1} b_i u_i$.
3. Στέλνει τὸν c στὸν Β.

[9] Ὁ κύριος S τοῦ RSA.

2.4.6 Ἀποκρυπτογράφηση

Ὁ Β χρησιμοποιεῖ τὸ μυστικὸ κλειδί του γιὰ νὰ ὑπολογίσει πρῶτα d_1, d_2, τέτοια ὥστε $d_1 a_1 \equiv 1 \pmod{n_1}$ καὶ $d_2 a_2 \equiv 1 \pmod{n_2}$ καὶ μετὰ τὸν ἀριθμὸ $N = [\, d_1 [d_2 c]_{n_2} \,]_{n_1}$. Τέλος, λύνει ἕνα πρόβλημα γυλιοῦ γιὰ τὴν ὑπεραύξουσα ἀκολουθία $(v_0, v_1, \ldots, v_{k-1})$ καὶ τὸν ἀριθμὸ N.

Ἀπόδειξη ὅτι ὁ Β θὰ ὑπολογίσει, τελικά, τὸν m. Εἶναι

$$[d_2 c]_{n_2} \equiv \sum_{i=0}^{k-1} b_i d_2 u_i \equiv \sum_{i=0}^{k-1} b_i d_2 (a_2 w_i) \equiv \sum_{i=0}^{k-1} b_i (d_2 a_2) w_i \equiv \sum_{i=0}^{k-1} b_i w_i \pmod{n_2} . \tag{3}$$

Ἐξ ὁρισμοῦ, $0 \le [d_2 c]_{n_2} < n_2$, ἐνῶ $\displaystyle\sum_{i=0}^{k-1} b_i w_i \le \sum_{i=0}^{k-1} w_i < k n_1 < n_2$. Ἄρα, μὲ συλλογισμὸ ὅμοιο μὲ αὐτόν, ποὺ κάναμε πρίν, τὸ ἀριστερώτερο καὶ τὸ δεξιώτερο μέλος τῆς (3) εἶναι ἴσα. Ἕπεται ὅτι

$$N \equiv d_1 \sum_{i=0}^{k-1} b_i w_i = \sum_{i=0}^{k-1} b_i d_1 w_i \sum_{i=0}^{k-1} b_i d_1 (a_1 v_i) \equiv \sum_{i=0}^{k-1} b_i (d_1 a_1) v_i \equiv \sum_{i=0}^{k-1} b_i v_i \pmod{n_1} .$$

Ὅπως πρίν, τὸ ἀριστερώτερο καὶ τὸ δεξιώτερο μέλος εἶναι ἴσα, ἄρα, ἐπιλύοντας ὁ Β τὸ πρόβλημα γυλιοῦ γιὰ τὴν ὑπεραύξουσα ἀκολουθία $(v_0, v_1, \ldots, v_{k-1})$ καὶ τὸν N, θὰ καταλήξει στὴν εὕρεση τῶν $b_{k-1}, \ldots, b_1, b_0$.

3 Κρυπτοσυστήματα δημοσίου κλειδιοῦ μὲ ἐλλειπτικὲς καμπύλες

Ἡ ἀσφάλεια αὐτῶν τῶν κρυπτοσυστημάτων βασίζεται στὸ ὅτι τὸ πρόβλημα 1.2.2 εἶναι ἀκόμη δυσκολότερο ἀπὸ τὸ πρόβλημα 1.1.2 (βλ. πρὸς τὸ τέλος τῆς παραγράφου 1.2).

Στὸ πρῶτο ἀπὸ τὰ κρυπτοσυστήματα, ποὺ θὰ παρουσιάσομε, τὸ πρὸς κρυπτογράφηση μήνυμα "ἀναπαριστάνεται" πρῶτα ἀπὸ ἕνα σημεῖο ἐλλειπτικῆς καμπύλης. Στὸ δεύτερο κρυπτοσύστημα, τὸ πρὸς κρυπτογράφηση μήνυμα εἶναι στοιχεῖο $(m_1, m_2) \in \mathbb{F}_p \times \mathbb{F}_p$, τὸ ὁποῖο, ἐν γένει, δὲν ἀνήκει στὴν καμπύλη (δηλαδή, δὲν ἀνήκει, κατ' ἀνάγκη στὴν ὁμάδα $\tilde{E}(\mathbb{F}_p)$, ἀλλά, κατὰ κάποιον τρόπο, "καμουφλάρεται" ἀπὸ ἕνα σημεῖο τῆς καμπύλης.

Καὶ στὶς δύο περιπτώσεις, ἡ ἐλλειπτικὴ καμπύλης E μὲ ἐξίσωση $y^2 = x^3 + ax + b$ $(a, b \in \mathbb{Z})$ καὶ ὁ πρῶτος p εἶναι *παράμετροι τοῦ συστήματος ἐπικοινωνίας*, δηλαδή, ὅλες οἱ ἐπικοινωνοῦσες ὀντότητες χρησιμοποιοῦν

τὴν ἴδια καμπύλη E καὶ τὸν ἴδιο πρῶτο p. Ὁ πρῶτος p ἐπιλέγεται, ὅπως πάντα, ἔτσι ὥστε ἡ ἀναγωγὴς τῆς καμπύλης $E \bmod p$ νὰ εἶναι ἐλλειπτική, ἰσοδύναμα, ἔτσι ὥστε ὁ p νὰ μὴ διαιρεῖ το᾽ν $4a^3 + 27b^2$.

3.1 Ἀναπαράσταση τῶν στοιχείων τοῦ $\mathbb{F}_p$ ἀπὸ σημεῖα τῆς $E(\mathbb{F}_p)$

Τὰ πρὸς κρυπτογράφηση μηνύματα μετατρέπονται σὲ φυσικοὺς ἀριθμοὺς m μικρότερους ἀπὸ κάποιο φρᾶγμα N. Ἐπιλέγεται μία "μικρὴ" σταθερὰ κ, π.χ. $\kappa = 30$, τέτοια ὥστε, $\kappa N < p$. Οἱ ἀριθμοὶ N καὶ κ, ὅπως καὶ ἡ ἐλλειπτικὴ καμπύλη E καὶ ὁ πρῶτος p, εἶναι παράμετροι τοῦ συστήματος (βλ. λίγες γραμμὲς πιὸ πάνω).

Ἡ ἐπιλογὴ τοῦ σημείου $\tilde{E}(\mathbb{F}_p)$, τὸ ὁποῖο θὰ ἀναπαραστήσει ἕνα δεδομένο θετικὸ ἀκέραιο $m < N$, γίνεται ὡς ἑξῆς. Ἐπιλέγεται $j \in \{1, \ldots, \kappa\}$, τέτοιο ὥστε τὸ $(\kappa m + j)^3 + a(\kappa m + j) + b \in \mathbb{F}_p$ νὰ εἶναι τετράγωνο στὸ $\mathbb{F}_p$, δηλαδή, ἴσο μὲ λ^2 γιὰ κάποιο $\lambda \in \mathbb{F}_p$. Τὸ σημεῖο $(\kappa m + j, \lambda)$ ἀποτελεῖ τὴν ἀναπαράσταση τοῦ m πάνω στὴν καμπύλη $\tilde{E}$. Ἕνα φυσιολογικὸ ἐρώτημα, βέβαια, εἶναι, ἂν ὑπάρχει τέτοιο j. Ἡ ἀπάντηση εἶναι ὅτι, βάσει τοῦ σημαντικοῦ θεωρήματος τοῦ Hasse, ποὺ λέει ὅτι $|\tilde{E}(\mathbb{F}_p)| = p + 1 - a_p$ γιὰ κάποιον μὴ ἀρνητικὸ ἀκέραιο $a_p < 2\sqrt{p}$, ἀποδεικνύεται ὅτι, ἡ πιθανότητα νὰ βρεῖ κανεὶς ἕνα j ὅπως παραπάνω, εἶναι τουλάχιστον $1 - 2^{-\kappa}$, ἄρα εἴμαστε πρακτικῶς βέβαιοι γιὰ τὴν εὕρεση τοῦ j. Εἶναι εὔκολο νὰ ᾽δεῖ κανείς ὅτι $m = \lfloor \frac{\kappa m + j - 1}{\kappa} \rfloor$, ποὺ σημαίνει ὅτι, ἂν γνωρίζομε ὅτι ἕνα σημεῖο $(\tilde{x}, \tilde{y}) \in E(\mathbb{F}_p)$ ἀποτελεῖ ἀναπαράσταση κάποιου ἀριθμοῦ m, τότε $m = \lfloor \frac{\tilde{x}-1}{\kappa} \rfloor$. Αὐτὸ μᾶς ἐπιτρέπει, στὸ πρῶτο ἀπὸ τὰ παρακάτω κρυπτοσυστήματα, νὰ θεωροῦμε ὅτι τὰ πρὸς κρυπτογράφηση μηνύματα εἶναι σημεῖα τῆς $\tilde{E}(\mathbb{F}_p)$.

3.2 Κρυπτοσύστημα El Gamal μὲ ἐλλειπτικὴ καμπύλη

Πρόκειται γιὰ κρυπτοσύστημα, τοῦ ὁποίου ἡ ἀσφάλεια βασίζεται στὸ ἀνέφικτὸ τῆς πρακτικῆς ἐπιλύσεως τοῦ προβλήματος τοῦ διακριτοῦ λογαρίθμου σὲ ἐλλειπτικὴ καμπύλη (βλ. 1.2.2). Κάθε μία ἀπὸ τὶς ἐπικοινωνοῦσες ὀντότητες δημιουργεῖ ἕνα δημόσιο καὶ ἕνα ἰδιωτικὸ κλειδί.

3.2.1 Δημιουργία δημοσίου καὶ ἰδιωτικοῦ κλειδιοῦ

1. Ἐπιλέγει ἕνα σημεῖο P τῆς E, ἄπειρης τάξης, μὲ ρητὲς συντεταγμένες, τέτοιο ὥστε, οἱ παρονομαστὲς τῶν συντεταγμένων τοῦ P νὰ εἶναι πρῶ-

τοι πρὸς τὸν p (δηλαδή, $\tilde{P} \neq \tilde{\mathcal{O}}$). Μία ἀπολύτως ἀπαραίτητη ἐπιπλέον συνθήκη γιὰ τὸ P εἶναι, ἡ κυκλικὴ ὑποομάδα $\langle \tilde{P} \rangle$ τῆς $\tilde{E}(\mathbb{F}_p)$ νὰ ἔχει μεγάλη τάξη. Κάποια σχετικὰ σχόλια γίνονται παρακάτω, στὴν ἑνότητα 3.4.

2. Ἐπιλέγεται ἕνας φυσικὸς ἀριθμὸς t, μικρότερος ἀπὸ τὴν τάξη τοῦ $\tilde{P}$ καὶ ὑπολογίζεται τὸ σημεῖο $\tilde{Q} = t\tilde{P}$.

3. **Δημόσιο κλειδὶ** εἶναι τὸ $(\tilde{P}, \tilde{Q})$ καὶ **ἰδιωτικὸ κλειδὶ** τὸ t.

3.2.2 Κρυπτογράφηση

Ἡ Ἀνθή, γιὰ νὰ κρυπτογραφήσει καὶ νὰ στείλει στὸν Βασίλη τὸ μήνυμα-ἀριθμὸ m, ὅπου m θετικὸς ἀκέραιος $< N$, κάνει τὰ ἑξῆς :

1. Πληροφορεῖται τὸ δημόσιο κλειδὶ $(\tilde{P}, \tilde{Q})$ τοῦ Βασίλη.

2. Ἀναπαριστᾷ τὸ m ἀπὸ σημεῖο $\tilde{M} \in \tilde{E}(\mathbb{F}_p)$ (βλ. ἑνότητα 3.1).

3. Ἐπιλέγει φυσικὸ ἀριθμὸ ν καὶ ὑπολογίζει τὰ σημεῖα $C_1 = \nu\tilde{P} \in \tilde{E}(\mathbb{F}_p)$ καὶ $C_2 = \tilde{M} + \nu\tilde{Q} \in \tilde{E}(\mathbb{F}_p)$.

4. Τὸ κρυπτογραφημένο μήνυμα, ποὺ στέλνει ἡ Ἀνθὴ στὸν Βασίλη, εἶναι τὸ (C_1, C_2).

3.2.3 Ἀποκρυπτογράφηση

Ὅταν ὁ Βασίλης λάβει τὸ (C_1, C_2), ὑπολογίζει τὸ $C_2 - tC_1$ καὶ βρίσκει τὸ $\tilde{M}$. Πράγματι, $C_2 - tC_1 = \tilde{M} + \nu(t\tilde{P}) - t(\nu\tilde{P}) = \tilde{M}$. Ξέροντας τὸ $\tilde{M}$, μπορεῖ, πολὺ εὔκολα νὰ ὑπολογίσει τὸ m, καθὼς εἴπαμε στὴν ἑνότητα 3.1.

Ἄσκηση 7. *Ἂν ἡ Ἀνθὴ στέλνει πολλὰ κρυπτογραφημένα μηνύματα m στὸν Βασίλη, γιατὶ πρέπει, γιὰ κάθε m νὰ ἐπιλέγει διαφορετικὴ παράμετρο ν;*

Ἄσκηση 8. Ἄσκηση. *Στὴν ἑνότητα 2.3 περιγράψαμε τὸ "κλασικὸ" κρυπτοσύστημα El Gammal. Συγκρίνετέ το μὲ τὸ κρυπτοσύστημα El Gamal μὲ ἐλλειπτικὴ καμπύλη καὶ βρεῖτε τὰ κοινὰ χαρακτηριστικά τους. Περιγρᾶψτε ὕστερα τὸ γενικὸ κρυπτοσύστημα El Gamal, δηλαδή, αὐτὸ ποὺ χρησιμοποιεῖ μιὰ γενικὴ ὁμάδα $(G, \cdot)$. Πῶς πρέπει κανεὶς νὰ ἐπιλέξει τὴν G ὥστε τὸ κρυπτοσύστημα νὰ εἶναι ἀσφαλές;*

3.3 Κρυπτοσύστημα Ἐλλειπτικῆς Καμπύλης τῶν Menezes-Vanstone

Σὲ αὐτὸ τὸ κρυπτοσύστημα ὁ ρόλος τῆς ἐλλειπτικῆς καμπύλης δὲν εἶναι νὰ κωδικοποιεῖ τὰ μηνύματα πρὶν ἀπὸ τὴν κρυπτογράφησή τους, ἀλλὰ νὰ τὰ "καμουφλάρει". Τὰ μηνύματα τώρα εἶναι στοιχεῖα τῆς $\mathbb{F}_p^* \times \mathbb{F}_p^*$.

Κάθε μία ἀπὸ τὶς ἐπικοινωνοῦσες ὀντότητες δημιουργεῖ ἕνα δημόσιο καὶ ἕνα ἰδιωτικὸ κλειδί ὡς ἑξῆς.

3.3.1 Δημιουργία δημοσίου καὶ ἰδιωτικοῦ κλειδιοῦ

1. Ἐπιλέγει σημεῖο P τῆς E μὲ ἀκέραιες συντεταγμένες, τέτοιο ὥστε τὸ $\tilde{P} \in \tilde{E}(\mathbb{F}_p)$ νὰ ἔχει μεγάλη τάξη· βλ. παρακάτω, ἑνότητα 3.4.

2. Ἐπιλέγει φυσικὸ ἀριθμὸ t μικρότερο ἀπὸ τὴν τάξη τοῦ $\tilde{P}$ καὶ ὑπολογίζει τὸ $\tilde{Q} = t\tilde{P}$.

3. **Δημόσιο κλειδὶ** εἶναι τὸ $\tilde{P}, \tilde{Q}$) καὶ **ἰδιωτικὸ κλειδὶ** τὸ t.

3.3.2 Κρυπτογράφηση

Ὅταν ἡ Ἀνθὴ θέλει νὰ στείλει στὸν Βασίλη κρυπτογραφημένο μήνυμα, κάνει τὰ ἑξῆς :

1. Πληροφορεῖται τὸ δημόσιο κλειδὶ $(\tilde{P}, \tilde{Q})$ τοῦ Βασίλη.

2. Ἐπιλέγει ἕνα φυσικὸ ἀριθμὸ k καὶ ὑπολογίζει τὸ $\tilde{R} = k\tilde{P}$ καὶ τὸ $k\tilde{Q}$=(ἔστω) (x_0, y_0), γιὰ κάποια $x_0, y_0 \in \mathbb{F}_p^*$. Εἶναι εὔκολο νὰ ἀποφύγει τιμὲς τοῦ k, ποὺ θὰ τὶς ἔδιναν x_0 ἢ y_0 ἴσο μὲ $0 \in \mathbb{F}_p$.

3. Γιὰ κάθε μήνυμά της $(m_1, m_2) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ ὑπολογίζει τὰ $c_1 = x_0 m_1 \in \mathbb{F}_p$ καὶ $c_2 = y_0 m_2 \in \mathbb{F}_p$.

4. Τὸ κρυπτογραφημένο μήνυμα, ποὺ στέλνει ἡ Ἀνθὴ στὸν Βασίλη, εἶναι τὸ (R, c_1, c_2).

3.3.3 Ἀποκρυπτογράφηση

Ὅταν ὁ Βασίλης λάβει τὸ (R, c_1, c_2) ὑπολογίζει τὸ $a\tilde{R}$ καὶ βρίσκει τὰ x_0, y_0. Πράγματι, $a\tilde{R} = a(k\tilde{P}) = k(a\tilde{P}) = k\tilde{Q} = (x_0, y_0)$. Στὴ συνέχεια, βρίσκει τὰ m_1, m_2 κάνοντας στὸ $\mathbb{F}_p^*$ τοὺς ὑπολογισμοὺς $c_1 x_0^{-1}$ καὶ $c_2 y_0^{-1}$.

3.4 Κάποια σχόλια γιὰ τὶς ἐλλειπτικὲς καμπῦλες πάνω ἀπὸ τὸ $\mathbb{F}_p$

Δύο εἶναι τὰ πολὺ σημαντικὰ θεωρήματα γιὰ τὴν τάξη $|\tilde{E}(\mathbb{F}_p)|$ τῆς ὁμάδας $|\tilde{E}(\mathbb{F}_p)|$. Ἀφ' ἑνός, ἰσχύει τὸ θεώρημα τοῦ Hasse, σύμφωνα μὲ τὸ ὁποῖο $|\tilde{E}(\mathbb{F}_p)| = p + 1 - a_p$ γιὰ κάποιο μὴ ἀρνητικὸ ἀκέραιο $a_p < 2\sqrt{p}$· ἀφ' ἑτέρου, ἰσχύει ὅτι ἡ ὁμάδα $\tilde{E}(\mathbb{F}_p)$ ἢ εἶναι κυκλική, ἢ $\tilde{E}(\mathbb{F}_p) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$, ὅπου $d_1|d_2$ καὶ $d_1|(p-1)$. [10] Ἀπὸ τὸ θεώρημα τοῦ Hasse βλέπομε ὅτι ἡ τάξη τῆς ὁμάδας $\tilde{E}(\mathbb{F}_p)$ "δὲν διαφέρει πολὺ" ἀπὸ τὸν p, ἄρα, ἂν ἡ ὁμάδα εἶναι κυκλική, τότε ὑπάρχει σημεῖο μεγάλης τάξεως (σὲ σχέση, πάντα, μὲ τὸν p). Στὴ δεύτερη περίπτωση, $|\tilde{E}(\mathbb{F}_p)| = d_1 d_2$ καὶ ἀναμένει κανεὶς ὁ d_1 νὰ εἶναι πολὺ μικρὸς (π.χ. ≤ 4) καί, συνεπῶς, ὁ d_2 νὰ εἶναι πολὺ μεγάλος.

Ἀπὸ τὰ ἁπλὰ αὐτὰ σχόλια διαπιστώνομε ὅτι, μεταξὺ τῶν ἄλλων, εἶναι ἀπαραίτητο νὰ μπορεῖ κανεὶς νὰ ὑπολογίσει τὴν τάξη $|\tilde{E}(\mathbb{F}_p)|$. Χάρη στὸν λεγόμενο *ἀλγόριθμο τοῦ R. Schoof, αὐτὸς ὁ ὑπολογισμὸς ἐπιτυγχάνεται σὲ πολυωνυμικὸ χρόνο.*

4 Ψηφιακὲς ὑπογραφές

Ὁ ρόλος τῶν ψηφιακῶν ὑπογραφῶν εἶναι νὰ "δένουν" κάποιον μὲ τὸ μήνυμα, ποὺ ἔστειλε. Δηλαδή, ἂν ἡ Α ἔστειλε ἕνα μήνυμα m στὸν Β, ὁ Β νὰ μπορεῖ νὰ βεβαιωθεῖ ὅτι τὸ m ἔχει ὑπογραφεῖ ἀπὸ τὴν Α, ἔτσι ὥστε ἡ Α νὰ μὴ μπορεῖ νὰ ἀρνηθεῖ ὅτι ὑπέγραψε τὸ m, ὅπως θὰ συνέβαινε ἂν ὑπέγραφε ἕνα ἐπίσημο ἔγγραφο σὲ συμβολαιογράφο.

Τὸ γενικὸ σχῆμα τοῦ προβλήματος, ποὺ μελετᾶμε σὲ ὁλόκληρη τὴν παράγραφο 4, μπορεῖ νὰ περιγραφεῖ, σχηματικά, ὡς ἑξῆς : Ἡ Α ὑπογράφει ἕνα μήνυμα, τὸ ὁποῖο ἀποστέλει σὲ ἕναν ἢ περισσότερους παραλῆπτες. Τὸ μήνυμα αὐτό, δὲν εἶναι, ἐν γένει, κρυπτογραφημένο. Ὁ Β, ποὺ εἶναι ἕνας ἀπὸ τοὺς παραλῆπτε, θέλει νὰ βεβαιωθεῖ ὅτι τὸ συγκεκριμένο μήνυμα ὄντως ὑπεγράφη ἀπὸ τὴν Α. Ἡ διαδικασία ὑπογραφῆς τοῦ μηνύματος πρέπει νὰ εἶναι τέτοια, ὥστε νὰ ἀποκλείει τὸ ἐνδεχόμενο νὰ στείλει ὁ Γ μήνυμα[11] *στὸν Β, τὸ ὁποῖο δὲν ὑπέγραψε ἡ Α, δηλαδή, πρέπει νὰ ἀποκλείει τὴν πλαστοπροσωπεία.*

Θὰ χρησιμοποιήσομε τοὺς ἑξῆς συμβολισμούς :

- $\mathcal{M}$ *εἶναι ὁ χῶρος ὅλων τῶν καθαρῶν μηνυμάτων.*
- $\mathcal{M}'$ *εἶναι ὁ χῶρος τῶν ὑπογραφομένων μηνυμάτων. Γιὰ λόγους, ποὺ θὰ ἐξηγήσομε παρακάτω, μία βασικὴ ἀρχὴ τῆς ψηφιακῆς ὑπογραφῆς εἶναι*

[10] Βλ. [1] Θεώρημα 7.1.8 καὶ Πρόταση 7.1.9.

[11] Ἀκόμη καὶ μήνυμα δίχως νόημα

νὰ μὴ ὑπογράφεται ἕνα μήνυμα $m \in \mathcal{M}$, ἀλλὰ κάποιο ὑποκατάστατό του $m' \in \mathcal{M}'$. Συχνά, τὸ $\mathcal{M}'$ εἶναι ὑποσύνολο τοῦ $\mathcal{M}$, ἀλλὰ αὐτὸ δὲν εἶναι ἀπαραίτητο.

- *$\mathcal{S}$ εἶναι ὁ χῶρος τῶν ὑπογραφῶν, συνήθως ἀράδα σταθεροῦ πλήθους bits. Ἡ ὑπογραφὴ δὲν εἶναι ἀνεξάρτητη ἀπὸ τὸ μήνυμα. Δηλαδή, δὲν λέμε π.χ. «s εἶναι ἡ ὑπογραφὴ τῆς A», ἀλλὰ «s εἶναι ἡ ὑπογραφὴ τῆς A στὸ μήνυμα m».*

Πρίν ὑπογράψομε ἕνα μήνυμα $m \in \mathcal{M}$, τὸ μετατρέπομε σὲ ἕνα στοιχεῖο $m' \in \mathcal{M}'$. Ἡ μετατροπὴ αὐτὴ γίνεται μὲ τὶς συναρτήσεις σύντμησης *(hash functions) ἢ τὶς* συναρτήσεις πλεονασμοῦ *(redundancy functions), ἀνάλογα μὲ τὸν τύπο ψηφιακῆς ὑπογραφῆς, ποὺ θὰ ἐπιλέξει κανείς.*

Συναρτήσεις σύντμησης *(Hash functions). Πρόκειται γιὰ δημοσίως γνωστὲς συναρτήσεις* $\mathrm{h} : \mathcal{M} \to \mathcal{M}'$, *ὅπου τὸ $\mathcal{M}'$ εἶναι σύνολο ἀράδων bits, οἱ ὁποῖες ἔχουν ἕνα πολὺ μικρὸ προκαθορισμένο μῆκος, συνήθως, τῆς τάξεως τῶν 150-200 bits . Οἱ συναρτήσεις* h *ἔχουν τὶς ἑξῆς ἰδιότητες :*
(α΄) **Εὐκολία ὑπολογισμοῦ***: Δοθέντος ἑνὸς ὁποιουδήποτε $x \in \mathcal{M}$, ὁ ὑπολογισμὸς τοῦ* $\mathrm{h}(x)$ *εἶναι πολὺ εὔκολος στὴν πράξη.*
(β΄) **Ἀνθεκτικότητα στὴν εὕρεση προεικόνας***: Ἂν εἶναι γνωστὸ κάποιο y στὸ πεδίο τιμῶν τῆς* h, *εἶναι πρακτικῶς ἀνέφικτο νὰ ὑπολογισθεῖ ἔστω καὶ ἕνα στοιχεῖο τοῦ συνόλου* $\mathrm{h}^{-1}(y)$.
(γ΄) **Ἀνθεκτικότητα στὴν εὕρεση δεύτερης προεικόνας***: Δοθέντος x στὸ πεδίο ὁρισμοῦ τῆς* h, *εἶναι πρακτικῶς ἀνέφικτο νὰ βρεῖ κανεὶς $x' \neq x$, τέτοιο ὥστε* $\mathrm{h}(x_1) = \mathrm{h}(x_2)$.
(δ΄) **Ἀνθεκτικότητα στὶς συγκρούσεις***: Παρὰ τὸ προφανὲς γεγονὸς ὅτι ἡ* h *δὲν εἶναι ἀμφιμονοσήμαντη, εἶναι ἐξαιρετικὰ ἀπίθανο, στὴν πράξη, νὰ ὑπολογίσει κανεὶς διαφορετικὰ x_1, x_2 στὸ πεδίο ὁρισμοῦ τῆς* h, *τέτοια ὥστε* $\mathrm{h}(x_1) = h(x_2)$.

Συναρτήσεις πλεονασμοῦ *(Redundancy functions). Πρόκειται γιὰ δημοσίως γνωστὲς* **1-1** *συναρτήσεις* $\mathrm{R} : \mathcal{M} \to \mathcal{M}'$, *ὅπου τὸ $\mathcal{M}'$ ἀποτελεῖται ἀπὸ ἀριθμοὺς (ἢ ἀράδες bits) μὲ πολὺ ἰδιαίτερες ἰδιότητες, ἔτσι ὥστε, τὰ στοιχεῖα τοῦ* $\mathrm{R}(\mathcal{M})$ *νὰ εἶναι, ἀπὸ πρακτικὴ ἄποψη, ἀναγνωρίσιμα πολὺ εὔκολα καὶ ἡ πιθανότητα ἕνας τυχαῖα ἐπιλεγμένος ἀριθμὸς (ἢ μία ἀράδα bits) τοῦ $\mathcal{M}'$ νὰ ἀνήκει στὸ* $\mathrm{R}(\mathcal{M})$, *εἶναι πρακτικῶς ἀμελητέα. Ἀφ' ἑτέρου, ὅμως, ὁ πρακτικὸς ὑπολογισμὸς τῶν τιμῶν τῆς* $\mathrm{R}^{-1} : \mathrm{R}(\mathcal{M}) \to \mathcal{M}$ *εἶναι εὔκολος.*
Γιὰ παράδειγμα, ἔστω ὅτι $\mathcal{M}$ εἶναι ὁ χῶρος ὅλων τῶν μηνυμάτων n-bits, καὶ $\mathcal{M}'$ ὁ χῶρος τῶν μηνυμάτων 2n-bits. Ἂν $m = b_1 b_2 \dots b_n \in \mathcal{M}$, τότε θὰ μπορούσαμε νὰ ὁρίσομε $\mathrm{R}(m) = b_1 b_2 \dots b_n b_1 b_2 \dots b_n$. *Ἐδῶ, δηλαδή, τὸ* $\mathrm{R}(\mathcal{M})$ *ἀποτελεῖται ἀπὸ ἀριθμοὺς ἀρτίου πλήθους bits, τῶν ὁποίων τὸ δεύτερο μισὸ τμῆμα εἶναι*

ἐπανάληψη τοῦ πρώτου μισοῦ. Ἡ πιθανότητα ἕνα τυχαῖο μήνυμα τοῦ $\mathcal{M}'$ *νὰ ἀνήκει στὸ* $\mathrm{R}(\mathcal{M})$ *εἶναι* 2^{-n}*, ἄρα ἐντελῶς ἀμελητέα, ἀφοῦ στὴν πράξη τὸ* n *εἶναι πολὺ μεγάλο.*

Φανταζόμαστε τώρα ἕνα δίκτυο ἐπικοινωνουσῶν ὀντοτήτων, οἱ ὁποῖες ἀνταλλάσουν μεταξύ τους ὑπογεγραμμένα μηνύματα.

Διαδικασία ὑπογραφῆς. *Βασίζεται σὲ μία δημοσίως γνωστὴ* συνάρτηση ὑπογραφῆς

$$\mathrm{S} : \mathcal{M}' \to \mathcal{S} ,$$

καὶ μία δημοσίως γνωστὴ συνάρτηση ἐπαλήθευσης

$$\mathrm{V} : \mathcal{M} \times \mathcal{S} \to \{\text{ΝΑΙ},\ \text{ΟΧΙ}\} ,$$

γιὰ τὶς ψηφιακὲς ὑπογραφὲς μὲ παράρτημα (βλ. ἑνότητα 4.1), ἢ

$$\mathrm{V} : \mathcal{S} \to \mathcal{M}' ,$$

γιὰ τὶς ψηφιακὲς ὑπογραφὲς ἀνακτωμένου μηνύματος (βλ. ἑνότητα 4.2). Γίνεται χρήση μιᾶς δημοσίως γνωστῆς συνάρτησης σύντμησης R *ἢ πλεονασμοῦ* h*, ἀνάλογα μὲ τὸν χρησιμοποιούμενο τύπο ψηφιακῆς ὑπογραφῆς.*
Γιὰ νὰ ὑπογράψει ἡ A *ἕνα μήνυμα* $m \in \mathcal{M}$*, ὑπολογίζει πρῶτα τὸ* $m' \in \mathcal{M}'$*, ὅπου* $m' = \mathrm{h}(m)$ *ἢ* $\mathrm{R}(m)$*, ἀναλόγως τοῦ εἴδους ψηφιακῆς ὑπογραφῆς. Ὕστερα ὑπολογίζει* $\mathrm{S}_A(m') = s \in \mathcal{S}$*. Ὁ ὑποδείκτης* A *στὴ συνάρτηση* S *δηλώνει τὸ γεγονὸς ὅτι ἡ* S *ἐξαρτᾶται ἀπὸ τὸ ἰδιωτικὸ κλειδὶ τῆς* A*.*

Ἡ A *στέλνει στὸν* B *τὸ* (m, s)*, ἂν τὸ εἶδος ψηφιακῆς ὑπογραφῆς εἶναι μὲ παράρτημα ἢ τὸ* s*, ἂν τὸ εἶδος ψηφιακῆς ὑπογραφῆς εἶναι ἀνακτωμένου μηνύματος.*

Διαδικασία ἐπαλήθευσης. *Ὁ* B*, ποὺ λαμβάνει τὸ ὑπογεγραμμένο μήνυμα τῆς* A*, ὑπολογίζει* $\mathrm{V}_A(m, s)$*, ἢ* $\mathrm{V}_A(s)$*, ἀνάλογα μὲ τὸ ἂν ἡ ψηφιακὴ ὑπογραφὴ εἶναι μὲ παράρτημα ἢ ἀνακτωμένου μηνύματος. Ἐδῶ, ὁ ὑποδείκτης* A *ὑποδηλώνει ὅτι ἡ συνάρτηση* V *ἐξαρτᾶται ἀπὸ τὸ δημόσιο κλειδὶ τῆς* A*. Στὴν πρώτη περίπτωση, ὁ* B *δέχεται τὴν αὐθεντικότητα τοῦ μηνύματος (ὅτι ὄντως τὸ μήνυμα ἔχει τὴ γνήσια ὑπογραφὴ τῆς* A*) ἂν, καὶ μόνο ἂν, ἡ τιμὴ εἶναι* ΝΑΙ*· στὴ δεύτερη περίπτωση ὁ* B *δέχεται τὸ μήνυμα ἂν, καὶ μόνο ἂν,* $\mathrm{V}_A(s) \in \mathrm{R}(\mathcal{M})$*. Περισσότερες λεπτομέρειες δίνονται στὶς ἀντίστοιχες ἑνότητες 4.1 καὶ 4.2.*

Ἀπαραίτητη συνθήκη. *Οἱ συναρτήσεις* $\mathrm{S}, \mathrm{V}, \mathrm{h}$ *(ἢ* R*) πρέπει νὰ εἶναι τέτοιες ὥστε νὰ εἶναι πρακτικῶς ἀνέφικτη ἡ* ὑπαρκτὴ πλαστογράφηση.

Ὑπαρκτὴ πλαστογράφηση *(existential forgery). Λέμε ὅτι ἔχομε ὑπαρκτὴ πλαστογράφηση ἂν κάποιος διαφορετικὸς ἀπὸ τὴν* A *μπορεῖ νὰ βρεῖ*

$m \in \mathcal{M}$ *καὶ* $s \in \mathcal{S}$, *τέτοια ὥστε,* $\mathrm{V}_A(m, s) = \textsc{nai}$, *στὴν περίπτωση ὑπογραφῆς μὲ παράρτημα, ἢ* $\mathrm{V}_A(s) \in \mathrm{R}(\mathcal{M})$, *στὴν περίπτωση ὑπογραφῆς ἀνακτωμένου μηνύματος. Δηλαδή, ἡ ἐπαλήθευση θὰ βεβαιώσει ὅτι s εἶναι ὑπογραφὴ τῆς A στὸ μήνυμα m, ἐνῶ ἡ A οὐδέποτε ὑπ•γραψε τὸ m. Σημειῶστε ὅτι, γιὰ τὴν ὑπαρκτὴ πλαστογράφηση δὲν ἀπαιτεῖται τὸ m νὰ "ἔχει νόημα"· ἄλλωστε τὰ ὅρια μεταξὺ μηνυμάτων μὲ νόημα καὶ μηνυμάτων χωρὶς νόημα κάθε ἄλλο παρὰ σαφῆ εἶναι.*

Ἐπιθέσεις κατὰ τῆς ὑπογραφῆς. *Ὁ σχεδιαστὴς μιᾶς ψηφιακῆς ὑπογραφῆς πρέπει νὰ δώσει πολλὰ πλεονεκτήματα στὸν ἐπιτιθέμενο, δηλαδή, σ' αὐτὸν ποὺ ἐπιχειρεῖ νὰ πλαστοπροσωπήσει, γιὰ παράδειγμα, τὴν A. Πρέπει νὰ θεωρεῖ δεδομένο ὅτι ὁ ἐπιτιθέμενος ἔχει στὴ διάθεσή του ὑπογεγραμμένα μηνύματα* $m_1, m_2, \ldots$ *τῆς A μὲ τὶς ἀντίστοιχες ἔγκυρες ὑπογραφές τους. Ἐπίσης, πρέπει νὰ θεωρεῖ δεδομένο ὅτι ὁ ἐπιτιθέμενος ἔχει τὴ δυνατότητα νὰ ζητήσει ἀπὸ τὴν A νὰ τοῦ ὑπογράψει μήνυμα m, ποὺ ἐκεῖνος (ὁ ἐπιτιθέμενος) ἔχει ἐπιλέξει, χωρὶς ἡ A νὰ ὑποψιαστεῖ ὅτι αὐτὸ τῆς ζητεῖται μὲ "κακὸ σκοπό".*

Στὶς παραγράφους 4.1 καὶ 4.2 περιγράφονται σὲ γενικὲς γραμμὲς τὰ δύο βασικὰ σχήματα ψηφιακῆς ὑπογραφῆς καὶ ἐπισημαίνονται κάποιες ἀναγκαῖες συνθῆκες γιὰ τὴν ἀποφυγὴ ὑπαρκτῆς πλαστογράφησης. Στὴν παράγραφο 4.3 περιγράφονται πὶο συγκεκριμένα κάποια ἀπὸ τὰ ἐν χρήσει σχήματα.

4.1 Σχήματα ψηφιακῆς ὑπογραφῆς μὲ παράρτημα

Χαρακτηριστικό τους εἶναι ὅτι στὴν ἐπαλήθευση, ἐκτὸς ἀπὸ τὴν ὑπογραφή, εἶναι ἀπαραίτητο καὶ τὸ ἴδιο τὸ μήνυμα.

Εἶναι περισσότερο σὲ χρήση ἀπὸ τὰ σχήματα ἀνακτωμένου μηνύματος καὶ λιγότερο ἐπιρρεπῆ σὲ ὑπαρκτὴ πλαστογράφηση. Χρησιμοποιοῦνται γιὰ νὰ ὑπογράφουν μὴ ἀπόρρητα μηνύματα αὐθαιρέτου μήκους.

Ἡ μετατροπὴ τοῦ μηνύματος $m \in \mathcal{M}$ *σὲ ὑπογραφόμενο μήνυμα* $m' \in \mathcal{M}'$ *γίνεται μέσῳ μιᾶς δημοσίως γνωστῆς συνάρτησης σύντμησης* h.

Ἡ A, ποὺ θέλει νὰ στέλνει ὑπογεγραμμένα μηνύματα κάνει γνωστὸ σὲ ὅλους τὸ δημόσιο κλειδί της, μέσῳ τοῦ ὁποίου ἡ συνάρτηση ἐπαλήθευσης V *γίνεται ἡ δημοσίως γνωστὴ συνάρτηση ἐπαλήθευσης τῆς A, ποὺ συμβολίζομε* V_A. *Παράλληλα, ἡ συνάρτηση ὑπογραφῆς* S, *ποὺ ἐξαρτᾶται ἀπὸ τὸ ἰδιωτικὸ κλειδὶ τῆς A, γίνεατι ἡ ἰδιωτικὴ συνάρτηση ὑπογραφῆς τῆς A, ποὺ συμβολίζεται* S_A. *Οἱ δύο συναρτήσεις σχετίζονται ὡς ἑξῆς :*

$$\mathrm{V}_A(m, s) = \textsc{nai} \;\Leftrightarrow\; \mathrm{S}_A(\mathrm{h}(m)) = s\,. \tag{4}$$

Ἡ Α, ποὺ θέλει νὰ στείλει στὸν Β τὸ ὑπογεγραμμένο μήνυμα m, κάνει τὰ ἑξῆς : Ὑπολογίζει τὸ $m' = \mathrm{h}(m)$ *καὶ τὴν ὑπογραφὴ* $s = \mathrm{S}_A(m')$*, καὶ στέλνει τὸ* (m, s) *στὸν Β.*

Ὁ Β, ποὺ λαμβάνει τὸ (m, s) *ὑπολογίζει τὴν τιμὴ* $\mathrm{V}_A(m, s)$*. Τί θὰ βρεῖ; Ἂν δὲν ἔχει γίνει "ζαβολιά", ἰσχύει, ἐκ κατασκευῆς,* $s = \mathrm{S}_A(m') = \mathrm{S}_A(\mathrm{h}(m))$*, ἄρα, λόγῳ τῆς (4), θὰ βρεῖ* ΝΑΙ*. Ἂν, ὅμως, κάποιος, ποὺ δὲν ἔχει στὴ διάθεσή του τὸ ἰδιωτικὸ κλειδὶ τῆς Α, ὑπογράψει ἕνα μήνυμα m μὲ κάποια ὑπογραφὴ s, ἡ τιμὴ τῆς* $\mathrm{V}_A(m, s)$ *θὰ εἶναι* ΟΧΙ*, ὁπότε ὁ Β θὰ ἀπορρίψει τὸ μήνυμα.*

Ἄσκηση 9. *Γιατί, εἶναι ἀδύνατον γιὰ τὸν Γ, ὁ ὁποῖος δὲν ξέρει τὸ ἰδιωτικὸ κλειδὶ τῆς Α, νὰ φτιάξει μήνυμα m (ἔστω καὶ δίχως νόημα) καὶ ὑπογραφὴ s γιὰ τὸ m, τέτοια ὥστε* $\mathrm{V}_A(m, s) =$ ΝΑΙ*;*

Παρατηρῆστε ὅτι, τὸ ἰδιωτικὸ κλειδὶ χρησιμοποιεῖται μόνο γιὰ τὸν ὑπολογισμὸ τοῦ s καὶ μάλιστα, ὑπολογίζεται ὄχι μέσῳ τοῦ m, ἀλλὰ τοῦ πολὺ μικρότερου $m' = \mathrm{h}(m)$*. Αὐτὸ τὸ χαρακτηριστικό, ποὺ ἐπιτυγχάνεται χάρη στὴ χρήση τῆς συνάρτησης σύντμησης* h*, εἶναι ἕνα ἀκόμη πλεονέκτημα τῶν σχημάτων ψηφιακῆς ὑπογραφῆς μὲ παράρτημα.*

4.2 Σχήματα ψηφιακῆς ὑπογραφῆς ἀνακτωμένου μηνύματος

Χαρακτηριστικό τους εἶναι ὅτι, ἡ ὑπογραφὴ τοῦ μηνύματος ἀρκεῖ γιὰ νὰ τὸ ἀνακτήσει ὁ παραλήπτης καὶ νὰ ἐπαληθεύσει τὴν προέλευσή του. Χρησιμοποιοῦνται, κυρίως, γιὰ μηνύματα σταθεροῦ μήκους.

Ἡ μετατροπὴ τοῦ μηνύματος $m \in \mathcal{M}$ *σὲ ὑπογραφόμενο μήνυμα* $m' \in \mathcal{M}'$ *γίνεται μέσῳ μιᾶς συνάρτησης πλεονασμοῦ* R*.*

Ὅπως καὶ στὴν περίπτωση ὑπογραφῆς μὲ παράρτημα, ἡ Α, ποὺ θέλει νὰ στέλνει ὑπογεγραμμένα μηνύματα κάνει γνωστὸ σὲ ὅλους τὸ δημόσιο κλειδί της, μέσῳ τοῦ ὁποίου ἡ συνάρτηση ἐπαλήθευσης V *γίνεται δημοσίως γνωστὴ ὡς συνάρτηση ἐπαλήθευσης* V_A *τῆς Α. Παράλληλα, μέσῳ τοῦ ἰδιωτικοῦ κλειδιοῦ της, ἡ Α κατασκευάζει τὴν ἰδιωτική της συνάρτηση ὑπογραφῆς* S_A*. Οἱ δύο συναρτήσεις σχετίζονται ὡς ἑξῆς:*

$$\mathrm{V}_A \circ \mathrm{S}_A = \mathrm{id}_{\mathcal{M}'} .$$

Ἡ Α, ποὺ θέλει νὰ στείλει στὸν Β τὸ ὑπογεγραμμένο μήνυμα m, κάνει τὰ ἑξῆς : Ὑπολογίζει τὸ $m' = \mathrm{R}(m)$ *καὶ τὴν ὑπογραφὴ* $s = \mathrm{S}_A(m')$*, τὴν ὁποία στέλνει στὸν Β.*

Ὁ Β, ποὺ λαμβάνει τὴν ὑπογραφὴ s ἐξετάζει ἂν $\mathrm{V}_A(s) \in \mathrm{R}(\mathcal{M})$. *Ἂν ναί, δέχεται ὅτι τὸ μήνυμα ἔχει ὑπογραφεῖ ἀπὸ τὴν Α (εἶναι αὐθεντικὸ μήνυμα τῆς Α) καὶ τὸ ἀνακτᾶ ὑπολογίζοντας τὸ* $\mathrm{R}^{-1}(V_A(s))$. *Ἂν ὄχι, ἀπορρίπτει τὴν ὑπογραφή.*

Ἄσκηση 10. *Ἔστω ὅτι ἡ Α ὑπογράφει ἕνα μήνυμα μὲ ψηφιακὴ ὑπογραφὴ ἀνακτωμένου μηνύματος καὶ ἔστω s αὐτὴ ἡ ὑπογραφή, τὴν ὁποία στέλνει στὸν Β. Ἂς ποῦμε ὅτι ἐμεῖς, ὡς τρίτοι, ξέρομε μὲ βεβαιότητα ὅτι καμμιὰ "ζαβολιὰ" δὲν ἔγινε στὴ διαδρομὴ ἀπὸ τὴν Α στὸν Β. Ἐξηγῆστε, γιατὶ εἶναι βέβαιο ὅτι ὁ Β θὰ ἀποδεχτεῖ τὸ μήνυμα;*

Ἀναγκαιότητα χρήσεως τῆς R. *Ἂν ἡ Α ὑπογράφει τὰ στοιχεῖα τοῦ* $\mathcal{M}$, *δηλαδή, ἂν* $\mathcal{M}' = \mathcal{M}$ *καὶ ἡ* R *εἶναι ἡ ταυτοτικὴ συνάρτηση τοῦ* $\mathcal{M}$, *τότε ἔχομε φαινόμενα ὑπαρκτῆς πλαστογραφίας εἰς βάρος της, ὡς ἑξῆς: Ὁ Γ ἐπιλέγει αὐθαίρετο* $s \in \mathcal{S}$ *καὶ ὑπολογίζει τὸ* $\mathrm{V}_A(s) = m$, *ἔστω. Αὐτὸ μπορεῖ νὰ τὸ κάνει, διότι ἡ συνάρτηση* V_A *εἶναι δημοσίως γνωστή. Προσποιούμενος τὴν Α, στέλνει στὸν Β τὴν ὑπογραφὴ s. Ὁ Β ἐπαληθεύει ὅτι* $\mathrm{V}_A(s) = m \in \mathcal{M} = \mathrm{R}(\mathcal{M})$ *καὶ ἐξαπατᾶται δεχόμενος ὅτι τὸ m προῆλθε ἀπὸ τὴν Α. Ἀνάλογη ὑπαρκτὴ πλαστογραφία θὰ μποροῦσε νὰ συμβεῖ ἀκόμη κι ἂν ἡ* R *δὲν εἶναι ἡ ταυτοτικὴ ἀπεικόνιση τοῦ* $\mathcal{M}$, *ἐφ' ὅσον δὲν γίνει πολὺ προσεκτικὴ ἐπιλογὴ τῆς* R· *βλ. σχετικὰ § 11.3.2 (ii) καὶ παράδειγμα 11.21 στὸ [1], σὲ συνδυασμὸ μὲ τὴν παράγραφο 4.3.2.*

4.2.1 Ἀπὸ ψηφιακὴ ὑπογραφὴ ἀνακτωμένου μηνύματος σὲ ψηφιακὴ ὑπογραφὴ μὲ παράρτημα

Ἔστω ὅτι ἡ Α ἔχει στὴ διάθεσή της ἕνα σχῆμα ψηφιακῆς ὑπογραφῆς ἀνακτωμένου μηνύματος, ὅπως περιγράψαμε παραπάνω. Μὲ τὴ βοήθεια μιᾶς συνάρτησης σύντμησης h *μπορεῖ νὰ τὸ μετατρέψει σὲ σχῆμα ψηφιακῆς ὑπογραφῆς μὲ παράρτημα, ὡς ἑξῆς: Ἂν θέλει νὰ ὑπογράψει τὸ* $m \in \mathcal{M}$ *καὶ νὰ τὸ στείλει στὸν Β, ὑπολογίζει πρῶτα τὸ* $\mathrm{R}(\mathrm{h}(m)) = m'$ *καὶ ὕστερα ὑπολογίζει τὴν ὑπογραφὴ* $\mathrm{S}_A(m') = s$. *Στέλνει στὸν Β τὸ* (m, s).

Ὁ Β λαμβάνει τὸ (m, s) *καὶ κάνει τὰ ἑξῆς: Ἐξετάζει ἂν* $\mathrm{V}_A(s)$ *ἀνήκει στὸ πεδίο τιμῶν τῆς* R. *Ἂν ὄχι, δὲν δέχεται τὸ μήνυμα· ἂν ναί, προχωρεῖ, ὑπολογίζοντας τὰ* $\mathrm{R}^{-1}(\mathrm{V}_A(s))$ *καὶ* $\mathrm{h}(m)$. *Ἂν εἶναι διαφορετικά, ἀπορρίπτει τὸ μήνυμα· ἂν εἶναι ἴσα, τὸ δέχεται.*

Ἡ συνάρτηση πλεονασμοῦ παύει πιὰ νὰ εἶναι κρίσιμης σημασίας καὶ μπορεῖ νὰ ἐπιλεγεῖ γιὰ τὸν ρόλο αὐτὸ ὁποιαδήποτε ἀμφιμονοσήμαντη συνάρτηση $\mathrm{R} : \mathrm{h}(\mathcal{M}) \to \mathcal{M}'$, *γιὰ τὴν ὁποία οἱ τιμὲς τῆς* R^{-1} *ὑπολογίζονται εὔκολα.*

Ἄσκηση 11. *Ἔστω ὅτι ἡ Α ὑπογράφει ἕνα μήνυμα μὲ τὸν παραπάνω τρόπο ἕνα μήνυμα m καὶ ἔστω s αὐτὴ ἡ ὑπογραφή. Ὕστερα στέλνει στέλνει τὸ*

(m, s) *στὸν Β. Ἂς ποῦμε ὅτι ἐμεῖς, ὡς τρίτοι, ξέρομε μὲ βεβαιότητα ὅτι καμμιὰ "ζαβολιὰ" δὲν ἔγινε στὴ διαδρομὴ ἀπὸ τὴν Α στὸν Β. Ἐξηγῆστε γιατὶ εἶναι βέβαιο ὅτι ὁ Β θὰ ἀποδεχτεῖ τὸ μήνυμα;*

4.3 Διάφορα συγκεκριμένα σχήματα ψηφιακῆς ὑπογραφῆς

Σὲ αὐτὴ τὴν παράγραφο περιγράφομε πῶς ἐξειδικεύονται τὰ γενικὰ σχήματα ψηφιακῆς ὑπογραφῆς 4.1 καὶ 4.2 σὲ διάφορα συγκεκριμένα σχήματα.

4.3.1 Σχῆμα ὑπογραφῆς RSA μὲ παράρτημα

Ἡ ἀσφάλειά του βασίζεται στὴν πρακτικὴ ἀδυναμία ἐπίλυσης τοῦ προβλήματος RSA· βλ. (1) στὴν ἑνότητα 2.1.4. Κάνει χρήση συνάρτησης σύντμησης h.

Ἡ Α, ποὺ θέλει νὰ στέλνει ὑπογεγραμμένα μηνύματα, ἐπιλέγει δύο τυχαίους πολὺ μεγάλους πρώτους p, q, τοὺς ὁποίους κρατᾶ μυστικούς. Ὑπολογίζει τοὺς ἀριθμοὺς $n = pq, \phi = \phi(n) = (p-1)(q-1)$, ἐπιλέγει ἕνα τυχαῖο e πρῶτο πρὸς τὸ ϕ καί, τέλος, ὑπολογίζει d, τέτοιο ὥστε, $ed \equiv 1 \pmod{\phi}$. Δημοσιεύει τοὺς ἀριθμοὺς n καὶ e. Σὲ αὐτὸ τὸ σχῆμα, τὰ $\mathcal{M}, \mathcal{M}'$ εἶναι ὑποσύνολα τοῦ $\mathbb{Z}_n$ καὶ $\mathcal{S} = \mathbb{Z}_n$.

Ἐπιλέγεται ἡ συνάρτηση σύντμησης $\mathrm{h} : \mathcal{M} \to \mathcal{M}'$ *καὶ εἶναι δημοσίως γνωστή.*

Μυστικὴ συνάρτηση ὑπογραφῆς τῆς Α εἶναι ἡ $\mathrm{S}_A(m') = [m'^d]_n$.

Δημοσίως γνωστὴ συνάρτηση ἐπαλήθευσης εἶναι ἡ

$$\mathrm{V}_A(m, s) = \begin{cases} \text{ΝΑΙ}, & \text{ἂν } [s^e]_n = \mathrm{h}(m) \\ \text{ΟΧΙ}, & \text{διαφορετικά} \end{cases}$$

Ἡ Α, ποὺ θέλει νὰ στείλει στὸν Β τὸ μήνυμα $m \in \mathbb{Z}_n$ ὑπογεγραμμένο, ὑπολογίζει τὰ $m' = \mathrm{h}(m)$ καὶ $s = \mathrm{S}_A(m')) = [m'^d]_n$ καὶ στέλνει στὸν Β τὸ (m, s). Ὅταν ὁ Β λάβει τὸ μήνυμα (m, s) δὲν ἔχει παρὰ νὰ ὑπολογίσει $\mathrm{V}_A(m, s)$. Ἂν ἡ τιμὴ εἶναι ΝΑΙ*, δέχεται τὸ μήνυμα, διαφορετικά, τὸ ἀπορρίπτει.*

Ἄσκηση 12. *Ἐξηγῆστε γιατὶ εἶναι πρακτικῶς ἀνέφικτη ἡ ὑπαρκτὴ πλαστογράφηση στὴν ὑπογραφὴ RSA μὲ παράρτημα.*

Τώρα μποροῦμε νὰ δοῦμε πόσο ἀπολύτως κρίσιμες εἶναι οἱ ἀπαιτήσεις ποὺ θέσαμε στὴν ἑνότητα 4 γιὰ τὶς συναρτήσεις σύντμησης.

• *Ἂν ἡ* h *δὲν εἶναι ἀνθεκτικὴ στὴν εὕρεση προεικόνας, τότε μπορεῖ νὰ συμβεῖ τὸ ἑξῆς: Ὁ Γ ἔχει στὴν κατοχή του δύο μηνύματα* m_1, m_2 *τῆς Α μὲ τὶς ἀντίστοιχες αὐθεντικὲς ὑπογραφές τους* s_1, s_2. *Ὑπολογίζει* $m'_1 = \mathrm{h}(m_1)$, $m'_2 = \mathrm{h}(m_2)$ *καὶ* $m \in \mathrm{h}^{-1}(m'_1 m'_2)$. *Εἶναι ἁπλῆ ἄσκηση νὰ δεῖ κανεὶς ὅτι* $s_1 s_2$ *εἶναι ἔγκυρη ὑπογραφὴ τῆς Α στὸ* m, *ἐνῶ ἡ Α οὐδέποτε ὑπέγραψε τὸ* m.

• *Ἂν ἡ* h *δὲν εἶναι ἀνθεκτικὴ στὴν εὕρεση δεύτερης προεικόνας, τότε ὁ Γ ἐπιλέγει μήνυμα* m *τῆς ἀρεσκείας του καὶ μετὰ μπορεῖ νὰ ἐπιλέξει* $m_1 \neq m$, *τέτοιο ὥστε* $\mathrm{h}(m_1) = \mathrm{h}(m)$. *Ζητᾶ κατόπιν ἀπὸ τὴν Α νὰ τοῦ ὑπογράψει τὸ* m_1 *καὶ ἡ Α τοῦ τὸ ὑπογράφει μὲ τὴν ὑπογραφή,* $\acute{\epsilon}\sigma\tau\omega$, s. *Εἶναι ἁπλῆ ἄσκηση νὰ δεῖ κανεὶς ὅτι* s *εἶναι ἔγκυρη ὑπογραφὴ τῆς Α στὸ* m, *ἐνῶ ἡ Α οὐδέποτε ὑπέγραψε τὸ* m.

• *Ἂν ἡ* h *δὲν εἶναι ἀνθεκτικὴ στὶς συγκρούσεις, τότε ὁ Γ μπορεῖ νὰ βρεῖ* m_1, m_2 *διαφορετικά, τέτοια ὥστε* $\mathrm{h}(m_1) = \mathrm{h}(m_2)$. *Ζητᾶ κατόπιν ἀπὸ τὴν Α νὰ τοῦ ὑπογράψει τὸ* m_1 *καὶ ἡ Α τοῦ τὸ ὑπογράφει μὲ τὴν ὑπογραφή,* $\acute{\epsilon}\sigma\tau\omega$, s. *Τότε, ἐντελῶς ἀνάλογα μὲ τὴν προηγούμενη περίπτωση, βλέπει κανεὶς εὔκολα ὅτι* s *εἶναι ἔγκυρη ὑπογραφὴ τῆς Α στὸ* m_2, *ἐνῶ ἡ Α οὐδέποτε ὑπέγραψε τὸ* m_2.

4.3.2 Σχῆμα ὑπογραφῆς RSA ἀνακτωμένου μηνύματος

Ἡ ἀσφάλειά του βασίζεται στὴν πρακτικὴ ἀδυναμία παραγοντοποιήσεως ἑνὸς μεγάλου ἀκεραίου. Κάνει χρήση συνάρτησης πλεονασμοῦ R.

Ἡ Α, ποὺ θέλει νὰ στέλνει ὑπογεγραμμένα μηνύματα, ἐπιλέγει δύο τυχαίους πολὺ μεγάλους πρώτους p, q, *τοὺς ὁποίους κρατᾶ μυστικούς. Ὑπολογίζει τοὺς ἀριθμοὺς* $n = pq, \phi = \phi(n) = (p-1)(q-1)$, *ἐπιλέγει ἕνα τυχαῖο* e *πρῶτο πρὸς τὸ* ϕ *καί, τέλος, ὑπολογίζει* d, *τέτοιο ὥστε,* $ed \equiv 1 \pmod{\phi}$. *Δημοσιεύει τοὺς ἀριθμοὺς* n *καὶ* e. *Σὲ αὐτὸ τὸ σχῆμα, τὰ* $\mathcal{M}, \mathcal{M}'$ *εἶναι ὑποσύνολα τοῦ* $\mathbb{Z}_n$ *καὶ* $\mathcal{S} = \mathbb{Z}_n$.

Ἐπιλέγεται ἡ συνάρτηση πλεονασμοῦ $\mathrm{R} : \mathcal{M} \to \mathcal{M}'$ *καὶ εἶναι δημοσίως γνωστή.*

Μυστικὴ συνάρτηση ὑπογραφῆς τῆς Α εἶναι ἡ $\mathrm{S}_A(m') = [m'^d]_n$.

Δημοσίως γνωστὴ συνάρτηση ἐπαλήθευσης εἶναι ἡ $\mathrm{V}_A(s) = [s^e]_n$.

Ἡ Α, ποὺ θέλει νὰ στείλει στὸν Β τὸ μήνυμα $m \in \mathbb{Z}_n$ *ὑπογεγραμμένο, ὑπολογίζει τὸ* $m' = \mathrm{R}(m)$ *καὶ τοῦ στέλνει τὸ* $s = \mathrm{S}_A(m')) = [m'^d]_n$.

Ὁ Β, λαμβάνει τὸ s *καὶ ἐξετάζει ἂν* $\mathrm{V}_A(s) \in \mathrm{R}(\mathcal{M})$, *δηλαδή, ἂν* $[s^e]_n \in \mathrm{R}(\mathbb{Z}_n)$. *Ἂν ναί, τὸ δέχεται καὶ βρίσκει τὸ* m *ὑπολογίζοντας τὴν τιμὴ* $\mathrm{R}^{-1}([s^e]_n)$.

Εἶναι πολὺ ἁπλὸ νὰ ᾽δεῖ κανεὶς ὅτι, ἂν ὁ Β ἔλαβε τὸ παραπάνω s, *καὶ αὐτὸ τὸ* s *ὄντως ὑπεγράφη ἀπὸ τὴν Α, τότε, ὑπολογίζοντας τὴν τιμὴ* $\mathrm{V}_A(s)$ *θὰ διαπιστώσει ὅτι ἀνήκει στὸ* $\mathrm{R}(\mathcal{M})$.

Ἂς ἐξετάσομε τώρα τὶ μπορεῖ νὰ ἐπιχειρήσει ὁ Γ γιὰ νὰ πλαστοπροσωπήσει τὴν Α. Τὸ μόνο, ποὺ μπορεῖ νὰ κάνει, εἶναι νὰ πάρει τυχαῖο $s \in \mathbb{Z}_n$ καὶ νὰ τὸ στείλει στὸν Β. Ἀλλὰ ὁ Β θὰ ὑπολογίσει τὸ $[s^e]_n$, καὶ εἶναι ἐξαιρετικὰ ἀπίθανο νὰ ἀνήκει αὐτὸ τὸ στοιχεῖο στὸ $\mathrm{R}(\mathcal{M})$ *διότι, ἐκ κατασκευῆς τῶν συναρτήσεων πλεονασμοῦ, τὸ ποσοστὸ τῶν στοιχείων τοῦ $\mathcal{M}'$, τὰ ὁποῖα ἀνήκουν στὸ* $\mathrm{R}(\mathcal{M})$ *εἶναι ἀμελητέο.*

Διάφορες τεχνικὲς λεπτομέρειες, ποὺ ἀφοροῦν στὴν πρακτικὴ ἐφαρμογὴ αὐτοῦ τοῦ σχήματος, περιγράφονται στὴν § 11.3.3 τοῦ [1].

4.3.3 Σχῆμα ὑπογραφῆς γενικευμένου DSA

Πρόκειται γιὰ ὑπογραφὴ μὲ παράρτημα. Τὰ ἀρχικὰ γράμματα DSA σημαίνουν Digital Signature Algorithm καὶ προτάθηκε τὸ 1991 ἀπὸ τὸ National Institute of Standards and Technology (NIST) τῶν ΗΠΑ. Πρόκειται γιὰ τὸ πρῶτο σχῆμα ψηφιακῆς ὑπογραφῆς, ποὺ ἀναγνωρίσθηκε ποτὲ ἀπὸ κράτος.

Ἡ ἀσφάλειά του βασίζεται στὴν πρακτικὴ ἀδυναμία ὑπολογισμοῦ τοῦ διακριτοῦ λογαρίθμου σὲ κατάλληλη πεπερασμένη ἀβελιανὴ ὁμάδα G. Ἀναγκαία συνθήκη γιὰ τὴν ἐπιλογὴ τῆς G εἶναι νὰ μὴ λύνεται στὴν πράξη τὸ πρόβλημα τοῦ ἐλλειπτικοῦ λογαρίθμου. Στὴν ἀρχικὴ βασικὴ μορφὴ τοῦ DSA, $G = \mathbb{F}_p^*$. Ἐδῶ παρουσιάζομε τὴ γενικευμένη ἐκδοχή του, γιὰ ὁποιαδήποτε ὁμάδα G, ὅπως παραπάνω.

Δημοσίως γνωστὲς παράμετροι (δηλαδή, χρησιμοποιούμενες ἀπὸ ὅλους τοὺς χρῆστες τῆς ψηφιακῆς ὑπογραφῆς) εἶναι ἡ ὁμάδα G καὶ στοιχεῖο της g, τοῦ ὁποίου ἡ τάξη εἶναι ἕνας πρῶτος $q > 2^{160}$. Ὁ q, δηλαδή, εἶναι ἀρκετά, ἀλλὰ ὄχι "ὑπερβολικὰ" μεγάλος πρῶτος. Σ' αὐτὸ τὸ σχῆμα, $\mathcal{M} = \mathbb{Z}$, $\mathcal{M}' = \mathbb{F}_q$ καὶ γίνεται χρήση μιᾶς συνάρτησης σύντμησης $\mathrm{h} : \mathcal{M} \to \mathcal{M}'$, *καθὼς καὶ μιᾶς βοηθητικῆς 1-1 συνάρτησης $f : \langle g \rangle \to \mathbb{Z}$, ἐπίσης δημοσίων παραμέτρων. Ἡ* h *ἀπαιτεῖται, ὅπως πάντα, νὰ ἱκανοποιεῖ τὶς ἀπαιτήσεις, οἱ ὁποῖες ἀναφέρθηκαν στὴν ἑνότητα 4, ἀλλὰ γιὰ τὴν f δὲν ἀπαιτεῖται τίποτε πέραν τοῦ νὰ εἶναι 1-1. Χῶρος ὑπογραφῶν εἶναι ὁ $\mathcal{S} = G \times \mathbb{F}_q$, ὅπου τὰ στοιχεῖα τοῦ $\mathbb{F}_q$ ταυτίζονται μὲ τὰ $0, 1, \ldots, q-1$.*

Ἡ Α ποὺ θέλει νὰ στέλνει ὑπογεγραμμένα μηνύματα, ἐπιλέγει τὸ ἰδιωτικό της κλειδὶ $a \in \{0, 1, \ldots, q-1\}$. Δημόσιο κλειδί της εἶναι τὸ $y = g^a \in G$. Ἡ ἰδιωτικὴ συνάρτηση ὑπογραφῆς δὲν ἐξαρτᾶται μόνο ἀπὸ τὸ ἰδιωτικὸ κλειδὶ a, ἀλλὰ καὶ ἀπὸ μία τυχαῖα ἐπιλεγμένη παράμετρο $k \in \mathbb{Z}$, ὅπου $(k, q) = 1$, ἡ ὁποία εἶναι διαφορετικὴ γιὰ κάθε ὑπογραφόμενο μήνυμα[12]*. Συγκεκριμένα, ἡ*

[12] Ἡ παράμετρος *k* θὰ μποροῦσε νὰ ὀνομαστεῖ καὶ ¿ef'hmero ¿idiwtik'o kleid'i.

S_A *ὁρίζεται ὡς ἑξῆς :*

$$\mathrm{S}_A(m') = (r, s) \in G \times \mathbb{F}_q\,, \quad \text{ὅπου } r = g^k \text{ καὶ } s = [k^{-1} \cdot (m' + af(r))]_q\,.$$

Ἔτσι, γιὰ νὰ ὑπογράψει ἡ A τὸ μήνυμα m, ποὺ θέλει νὰ στείλει στὸν B, ὑπολογίζει $m' = \mathrm{h}(m)$ *καὶ* $\mathrm{S}_A(m')$*, καὶ στέλνει τὸ* (m, r, s) *στὸν B.*

Ὅταν λάβει ὁ B τὸ (m, r, s)*, καὶ θέλει νὰ ἐλέγξει τὴν αὐθεντικότητά του, χρησιμοποιεῖ τὴ συνάρτηση ἐπαλήθευσης τῆς A:*

$$\mathrm{V}_A(m, r, s) = \begin{cases} \textsc{nai}, & \text{ἂν } r^s = g^{h(m)} y^{f(r)} \\ \textsc{oxi}, & \text{διαφορετικά} \end{cases} \qquad \text{(ἰσότητες στὸ } \mathbb{F}_p\text{)}$$

Ἄσκηση 13. *Ἔστω ὅτι ἡ A ὑπογράφει ἕνα μήνυμα m μὲ ψηφιακὴ ὑπογραφὴ El Gamal καὶ ἔστω* (r, s) *αὐτὴ ἡ ὑπογραφή. Στὴ συνέχεια στέλνει τὸ* (m, r, s) *στὸν B. Ἂς ποῦμε ὅτι ἐμεῖς, ὡς τρίτοι, ξέρομε μὲ βεβαιότητα ὅτι καμμιὰ "ζαβολιὰ" δὲν ἔγινε στὴ διαδρομὴ ἀπὸ τὴν A στὸν B. Ἐξηγῆστε, γιατὶ εἶναι βέβαιο ὅτι ὁ B θὰ ἀποδεχτεῖ τὸ μήνυμα;*

Ἄσκηση 14. *Ἔστω ὅτι ὁ Γ ἐπιχειρήσει νὰ πλαστοπροσωπήσει τὴν A, τῆς ὁποίας ἰδιωτικὸ κλειδὶ (ἄγνωστο στὸν Γ) εἶναι τὸ a καὶ δημόσιο κλειδὶ εἶναι τὸ* $y = g^a$*. Ἐπιχειρεῖ νὰ ὑπολογίσει* $m \in \mathcal{M}$ *καὶ* $(r, s) \in \mathcal{S}$*, τέτοια ὥστε* (r, s) *νὰ εἶναι ἔγκυρη ὑπογραφὴ τῆς A γιὰ τὸ m.*
(α΄) Ἐξηγῆστε γιατί θὰ ἀποτύχει, εἴτε ξεκινήσει ἐπιλέγοντας τυχαία τὴν παράμετρο k, εἴτε ἐπιλέγοντας τυχαῖα τὸ s. Ἐξηγῆστε γιατί, αὐτὸ τὸ δεύτερο ἐνδεχόμενο θὰ ὁδηγήσει τὸν Γ σὲ χειρότερο ἀδιέξοδο.

Ἄσκηση 15. *Ἡ ἄσκηση αὐτὴ δείχνει ὅτι, ὅταν στὴν ὑπογραφὴ DSA ἐπιλέξομε τὴν ὁμάδα G, πρέπει νὰ παραμείνομε "πιστοὶ" στὸ σύνολο, στὸ ὁποῖο θὰ ἀναπαριστάνονται τὰ στοιχεῖα της. Δηλαδή, ἂν τὰ στοιχεῖα τῆς ὁμάδας G ἀναπαριστάνονται ἀπὸ τὰ στοιχεῖα τοῦ συνόλου* Σ_G*,* [13] *τότε ἡ συνάρτηση ἐπαλήθευσης πρέπει νὰ τροποποιηθεῖ ἐλαφρῶς ὡς ἑξῆς :*

$$\mathrm{V}_A(m, r, s) = \begin{cases} \textsc{nai}, & \text{ἂν } r \in \Sigma_G \text{ καὶ } r^s = g^{h(m)} y^{f(r)} \\ \textsc{oxi}, & \text{διαφορετικά} \end{cases} \qquad \text{(ἰσότητες στὸ } \mathbb{F}_p\text{)}$$

Ἂς πάρομε τώρα $G = \mathbb{F}_p^*$*, ὅπου τὰ στοιχεῖα της ἀναπαριστάνονται ἀπὸ τοὺς ἀριθμοὺς* $\{1, \ldots, p-1\}$*. Ἔστω* $g \in \{1, \ldots, p-1\}$*, τοῦ ὁποίου ἡ τάξη εἶναι q, ὅπου ὁ q εἶναι ἕνας μεγάλος πρῶτος ἀριθμός. Φυσικά,* $q|(p-1)$*. Ἡ συνάρτηση*

[13] Γιὰ παράδειγμα, ἂν $G = \mathbb{F}_5^*$, τότε γιὰ τὸ Σ_G ὑπάρχουν ἄπειρες ἐπιλογές, ὅπως, $\{1, 2, 3, 4\}$, $\{-2, -1, 1, 2\}$, $\{31, 32, 33, 34\}$.

f παίρνομε αὐτὴν, ποὺ σὲ κάθε $g^x \in \langle g \rangle$ ἀντιστοιχεῖ τὸ $[g^x]_q \in \mathbb{Z}$. Ἰδοὺ ἕνα σενάριο πλαστογράφησης, ποὺ μπορεῖ νὰ συμβεῖ ἂν δὲν τροποποιήσομε τὴ συνάρτηση ἐπαλήθευσης V_A, ὅπως παραπάνω: Ἔστω ὅτι (r, s) εἶναι μία ἔγκυρη ὑπογραφὴ τῆς A στὸ μήνυμα m καὶ ὁ Γ, ποὺ θέλει νὰ πλαστογραφήσει τὴν A, ἔχει στην κατοχή του τὸ μήνυμα αὐτὸ καὶ τὴν ὑπογραφή του. Ἂν συμβεῖ, πρᾶγμα διόλου ἀπίθανο, νὰ εἶναι $(r\mathrm{h}(m), p-1) = 1$, τότε ὁ Γ ἐπιλέγει μήνυμα m_1 τῆς ἀρεσκείας του καὶ ὑπολογίζει $s_1 = [s\mathrm{h}(m_1)\mathrm{h}(m)^{-1}]_{p-1}$. Χάρη στὸ κινέζικο θεώρημα, ὑπολογίζει r_1, τέτοιο ὥστε $r_1 \equiv r \pmod p$ καὶ $r_1 \equiv [r]_q \mathrm{h}(m_1)\mathrm{h}(m)^{-1} \pmod{p-1}$. Ἀποδεῖξτε ὅτι ὁ Γ πέτυχε μὲ τὰ (m_1, r_1, s_1) μιὰ ὑπαρκτὴ πλαστογράφηση τῆς A καὶ ἐξηγῆστε γιατὶ συνέβη αὐτό.

Ἄσκηση 16. *(Σχῆμα ὑπογραφῆς Schnorr). Πρόκειται γιὰ παραλλαγὴ τοῦ DSA. Ἡ σημασία τῶν G, g, q, r, a, k, y εἶναι ἡ ἴδια μὲ αὐτὴν στὸ DSA. Ἀντί, ὅμως, ἡ συνάρτηση κατακερματισμοῦ* h *νὰ ἔχει πεδίο ὁρισμοῦ τὸ $\mathcal{M} = \mathbb{Z}$, ἔχει τὸ $\mathbb{Z} \times \langle g \rangle$, δηλαδή,* $\mathrm{h} : \mathbb{Z} \times \langle g \rangle \to \mathbb{F}_q$. *Ἡ ὑπογραφὴ στὸ μήνυμα m εἶναι τώρα $(e, s) \in \mathbb{F}_q \times \mathbb{F}_q$, ὅπου $e = \mathrm{h}(m, r)$ καὶ $s = [k + ae]_q$. Ἀποδεῖξτε ὅτι ὁ ἔλεγχος τῆς σχέσης $\mathrm{h}(m, g^s y^{-e}) = e$ ἀπὸ τὸν παραλήπτη τοῦ m πιστοποιεῖ τὴν ἐγκυρότητα τοῦ μηνύματος m. Νὰ ὁρίσετε τυπικὰ τὴν ἰδιωτικὴ συνάρτηση S_A καὶ τὴ δημόσια συνάρτηση V_A. Μπεῖτε στὴ θέση ἑνὸς ἐπίδοξου πλαστογράφου καὶ ἐξηγῆστε γιατὶ δὲν μπορεῖτε νὰ ἐπιτύχετε ὑπαρκτὴ πλαστογράφηση.*
Δῶστε ἕνα "βρεφικὸ" ἀριθμητικὸ παράδειγμα ὑπογραφῆς μὲ αὐτὸ τὸ σχῆμα, στὸ ὁποῖο $G = \mathbb{F}_p$ μὲ τὸν πρῶτο $p \in (50, 100)$ καὶ h *δικῆς σας κατασκευῆς (δίχως τὶς ἀπαιτήσεις τῶν συναρτήσεων κατάτμησης). Τὸ μήνυμά, ποὺ θα ὑπογράψετε, ἂς εἶναι κάποιος διψήφιος (στὸ δεκαδικὸ σύστημα) ἀκέραιος.*

4.3.4 Ὑπογραφὴ Rabin

Πρόκειται γιὰ ὑπογραφὴ ἀνακτωμένου μηνύματος. Ἡ ἀσφάλειά του βασίζεται στὴν πρακτικὴ ἀδυναμία εὑρέσεως τετραγωνικῶν ριζῶν mod$n$, *ὅταν ὁ n εἶναι σύνθετος ἀκέραιος ἀριθμὸς μὲ δύο, τουλάχιστον, πολὺ μεγάλους πρώτους διαιρέτες.*

Ἡ A, ποὺ θέλει νὰ στέλνει ὑπογεγραμμένα μηνύματα, ἐπιλέγει δύο τυχαίους πολὺ μεγάλους πρώτους p, q, τοὺς ὁποίους κρατᾶ μυστικούς, καὶ ὑπολογίζει τὸν $n = pq$, τὸν ὁποῖο δημοσιεύει. Σὲ αὐτὸ τὸ σχῆμα, $\mathcal{M} \subseteq \mathbb{Z}_n$, $\mathcal{M}' \subseteq \mathbb{Q}_n$, ὅπου $\mathbb{Q}_n$ συμβολίζει τὴν ὑποομάδα τῶν τετραγώνων τῆς $\mathbb{Z}_n^*$, ἄρα τὰ στοιχεῖα της εἶναι $\equiv x^2 \pmod n$ γιὰ κάποιο $x \in \mathbb{Z}_n^*$ (δηλαδή, $\gcd(x, n) = 1$). Ἐπίσης, $\mathcal{S} = \mathbb{Z}_n^*$. Ἐπιλέγεται ἡ συνάρτηση πλεονασμοῦ $\mathrm{R} : \mathcal{M} \to \mathcal{M}'$ καὶ εἶναι δημοσίως γνωστή.

Μυστικὴ συνάρτηση ὑπογραφῆς τῆς A εἶναι ἡ

$$\mathrm{S}_A(m') = \text{ὁ ἐλάχιστος } s \in \{1, \ldots, n-1\}, \text{ τέτοιος ὥστε } s^2 \equiv m' \pmod{n},$$

Δημοσίως γνωστὴ συνάρτηση ἐπαλήθευσης εἶναι ἡ $\mathrm{V}_A(s) = [s^2]_n$.

Ὁ B, ποὺ λαμβάνει τὸ $s \in \mathbb{S}$, *ἐλέγχει τὴν αὐθεντικότητά του (ἂν, δηλαδή, εἶναι ὄντως ἡ A ποὺ τὸ ὑπέγραψε) μέσῳ τῆς σχέσης* $\mathrm{V}_A(s) \in \mathrm{R}(\mathcal{M})$.

Ἄσκηση 17. *Ἀναφερόμενοι στὴν παραπάνω περιγραφή, ἀποδεῖξτε ὅτι, ἂν τὸ s εἶναι αὐθεντικό, τότε ὄντως* $\mathrm{V}_A(s) \in \mathrm{R}(\mathcal{M})$.

Ἂς ἐξετάσομε τώρα τὶ μπορεῖ νὰ ἐπιχειρήσει ὁ Γ γιὰ νὰ πλαστοπροσωπήσει τὴν A. Ἂν στείλει στὸν B ἕνα τυχαῖο $s \in \mathbb{Z}_n$, *ὡς δῆθεν προερχόμενο ἀπὸ τὴν A, εἶναι πρακτικῶς βέβαιο ὅτι δὲν θὰ ἱκανοποιεῖται ἡ συνθήκη* $[s^2]_n \in \mathrm{R}(\mathcal{M})$, *διότι τὸ ποσοστὸ τῶν στοιχείων τοῦ* $\mathrm{R}(\mathcal{M})$ *στὸ* $\mathcal{M}'$ *εἶναι ἀμελητέο. Ἂν, πάλι, πρῶτα ἐπιλέξει τὸ* $m \in \mathcal{M}$ *καὶ μετὰ ἐπιχειρήσει νὰ λύσει ὡς πρὸς s τὴν ἰσοδυναμία* $s^2 \equiv \mathrm{R}(m) \pmod{n}$, *τότε ἔχει νὰ ἀντιμετωπίσει τὸ ἐξαιρετικὰ δύσκολο, ἀπὸ ὑπολογιστικὴ ἄποψη, πρόβλημα τῆς εὑρέσεως τετραγωνικῆς ρίζας* $\bmod n$ *γιὰ σύνθετους n.*

Δὲν μπορεῖ νὰ ἐξασφαλισθεῖ μὲ βεβαιότητα ὅτι οἱ τιμὲς τῆς συνάρτησης πλεονασμοῦ R *πέφτουν πάντα μέσα στὸ* $\mathbb{Q}_n$. *Ἂν ἡ A, ποὺ θέλει νὰ ὑπογράψει τὸ* $m \in \mathcal{M}$, *διαπιστώσει ὅτι* $\mathrm{R}(m) \notin \mathbb{Q}_n$, *εἶναι ὑποχρεωμένη νὰ τὸ τροποποιήσει, δίχως νὰ τὸ ἀλλοιώσει οὐσιαστικά. Ὑπάρχουν διάφορες τεχνικές, ποὺ ἐφαρμοζόμενες μία ἢ περισσότερες φορὲς στὸ m, θὰ δώσουν μὲ πολὺ μεγάλη πιθανότητα, ἕνα τροποποιημένο μήνυμα* m_1, *τέτοιο ὥστε* $\mathrm{R}(m_1) \in \mathbb{Q}_n$ *καὶ ἡ γνώση τοῦ* m_1 *νὰ συνεπάγεται γνώση τοῦ m. Ἡ A, στὴ συνέχεια, ὑπογράφει τὸ* m_1 *ἀντὶ τοῦ m. Ὅταν ὁ B λάβει τὴν ὑπογραφὴ τοῦ* m_1, *βεβαιώνεται γιὰ τὴν αὐθεντικότητά της καὶ ἀνακτᾷ τὸ* m_1. *Κατ᾽οπιν, ἔχοντας τὸ* m_1, *ὑπολογίζει καὶ τὸ m.*

Γιὰ νὰ ἀντιμετωπισθεῖ αὐτὸ τὸ θέμα, ἔτσι ὥστε ἡ A νὰ εἶναι βέβαιη *ὅτι* $\mathrm{R}(m) \in \mathbb{Q}_n$, *ὑπάρχει ἡ* τροποποιημένη μέθοδος ὑπογραφῆς Rabin· *βλ.* §§ *11.27-11.32 στὸ [1].*

Ἄσκηση 18. *Δῶστε ἕνα "βρεφικὸ" παράδειγμα ὑπογραφῆς Rabin, ἀκολουθώντας τὶς ἑπόμενες γραμμές: Ἐπιλέξτε δύο διψήφιους πρώτους* p, q, *τέτοιους ὥστε* $n = pq > 1000$. *Ὑπολογῖστε μὲ τὴ βοήθεια ὑπολογιστῆ τὸ σύνολο* $\mathbb{Q}_n$. *Θεωρῆστε τὸ ὑπσύνολο* $\mathcal{M}'$ *τοῦ* $\mathbb{Q}_n$, *ποὺ ἀποτελεῖται ἀπὸ ἐκεῖνα ἀκριβῶς τὰ στοιχεῖα τοῦ* $\mathbb{Q}_n$ *μὲ τὴν ἰδιότητα τὰ ψηφία τους τῶν δεκάδων καὶ τῶν μονάδων νὰ εἶναι ἴσα. Ὡς* $\mathcal{M}$ *θεωρῆστε τὸ σύνολο τῶν μονοψηφίων ἢ*

διψηφίων ἀριθμῶν, ποὺ φτιάχνονται ἀπὸ τοὺς ἀριθμοὺς τοῦ $\mathcal{M}'$ *ὅταν τοὺς κόβομε τὸ ψηφίο τῶν μονάδων. Ἄρα* $\mathrm{R} : \mathcal{M} \to \mathcal{M}'$ *εἶναι ἡ συνάρτηση ποὺ τὸν δεκαδικὸ ἀριθμὸ* $\overline{b_1 b_0}$ *στέλνει στὸν* $\mathrm{R}(\overline{b_1 b_0}) = \overline{b_1 b_0 b_0}$*. Ἐπιλέξτε κάποια "μηνύματα"* $m \in \mathcal{M}$*, ὑπογράψτε τα καὶ μετὰ ἐπαληθεῦστε τὴν αὐθεντικότητά τους, σὰν νὰ εἴσαστε ἄλλος ἀπὸ αὐτὸν ποὺ τὰ ὑπέγραψε.*

Ἀναφορὲς

[1] H. Cohen, A course in Computational Algebraic Number Theory, *Graduate Texts in Mathematics 138, Springer 1995.*

[1] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of applied Cryptography, *CRC Press, Inc. 1997.*

[2] N. Koblitz, Algebraic aspects of Cryptography, *Algorithms and Computation in Mathematics, volume 3, Springer 1998.*

[3] N. Koblitz, A. Menezes, S. Vanstone, The state of Elliptic Curve Cryptography, Designs, Codes and Cryptography **19** *(2000), 173-193.*

[4] A. Shamir, *A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem,* IEEE Trans. Information Theory **30***, 699-704.*