ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ
ΣΗΜΕΙΩΣΕΙΣ #7

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

1. Το συστημα κρυπτογραφησης RSA

Σε δημοσίευση του 1978, οι Rivest, Shamir και Adleman πρότειναν σύστημα κρυπτογράφησης δημόσιου κλειδιού που φέρει τα αρχικά των ονομάτων τους. Ιστορικά ήταν το πρώτο σύστημα κρυπτογράφησης δημόσιου κλειδιού που έγινε δημοσιεύτηκε. Πολύ αργότερα έγινε γνωστό ότι το ίδιο ακριβώς σύστημα ήταν γνώστο στις βρετανικές μυστικές υπηρεσίες αρκετά χρόνια πριν.

Όπως σε κάθε σύστημα δημόσιου κλειδιού, κάθε χρήστης (που θέλει να λαμβάνει κρυπτογραφημένα μηνύματα) κατασκευάζει ένα ζευγάρι κλειδιών. Στο RSA επιλέγει δύο πρώτους αριθμούς p και q και υπολογίζει τα $n = pq$ και $\phi(n) = (p-1)(q-1)$. Επιπλέον επιλέγει τυχαίο ακέραιο $d \in [1, \phi(n)]$ με την ιδιότητα $(d, \phi(n)) = 1$ και υπολογίζει ακέραιο e που να ικανοποιεί την ισοτιμία $ed \equiv 1 \pmod{\phi(n)}$. Δηλαδή, ο e είναι ο αντίστροφος του d modulo $\phi(n)$ και μπορεί να υπολογιστεί εύκολα με τον επεκτεταμένο Ευκλείδειο αλγόριθμο. Το ιδιωτικό κλειδί είναι το d, ενώ το δημόσιο κλειδί είναι το (n, e). Παρατηρήστε ότι οι πρώτοι αριθμοί p, q δεν έχουν συμπεριληφθεί στο ιδιωτικό κλειδί. Ο λόγος είναι ότι οι πρώτοι δεν είναι απαραίτητοι για την αποκρυπτογράφηση. Φυσικά *πρέπει* να παραμείνουν μυστικοί: όποιος γνωρίζει τα p, q μπορεί να υπολογίσει το κρυφό κλειδί d όπως ακριβώς ο νόμιμος κάτοχος του κλειδιού.

Ο χώρος των καθαρών μηνυμάτων είναι οι ακέραιοι στο διάστημα $[1, n]$ που είναι πρώτοι προς το n. Είναι δηλαδή ένα ανηγμένο σύνολο υπολοίπων modulo n. Το κρυπτογράφημα ενός τέτοιου μηνύματος m έιναι το $c = m^e \mod n$. Όταν ο κάτοχος του ιδιωτικού κλειδιού παραλάβει το κρυπτογράφημα, υπολογίζει το καθαρό μήνυμα ως $m = c^d \mod n$. Η ορθότητα του συστήματος, δηλαδή το ότι ο αλγόριθμος της αποκρυπτογράφησης δίνει το καθαρό μήνυμα, είναι φανερή:

$$c^d \equiv m^{ed} \equiv m \pmod{n}.$$

Πριν εξετάσουμε την ασφάλεια του RSA, ας δούμε ένα παράδειγμα εφαρμογής του.

Παράδειγμα 1.1. Έστω ότι η Αλίκη θέλει να κατασκευάσει ένα ζευγάρι κλειδιών. Βρίσκει δύο πρώτους, έστω τους $p = 11$, $q = 13$ και υπολογίζει το γινόμενο τους $n = 11 \cdot 13 = 143$ και το $\phi(n) = \phi(143) = 10 \cdot 12 = 120$. Επιπλέον επιλέγει το (μυστικό) εκθέτη αποκρυπτογράφησης, έστω $d = 23$ και υπολογίζει τον

αντίστροφο του modulo n, δηλαδή υπολογίζει το $e = 47$. Το ιδιωτικό κλειδί της Αλίκης είναι το $d = 23$ και το δημόσιο κλειδί το $(n, e) = (143, 47)$. Έστω ότι ο Βασίλης θέλει να στείλει στην Αλίκη το μήνυμα $m = 15$. Υπολογίζει το

$$c = m^e \mod n = 15^{47} \mod 143 = 137.$$

Η Αλίκη λαμβάνει το κρυπτογράφημα και υπολογίζει

$$c^d \mod n = 137^{23} \mod 143 = 15,$$

που είναι το αρχικό μήνυμα.

2. Ασφαλεια

Για να μελετήσουμε την ασφάλεια του RSA θα μας βοηθήσει να ορίσουμε και να μελετήσουμε τα παρακάτω προβλήματα.

Πρόβλημα RSA (RSA). Δεδομένου φυσικού αριθμού n, ο οποίος είναι γινόμενο δύο περιττών πρώτων, φυσικού αριθμού e τέτοιου ώστε $(e, \phi(n)) = 1$ και ακεραίου b, να υπολογιστεί ακέραιος x τέτοιος ώστε $x^e \equiv b \pmod{n}$.

Πρόβλημα παραγοντοποίησης (FACTOR). Δεδομένου φυσικού αριθμού n, οποίος είναι γινόμενο δύο περιττών πρώτων, να υπολογιστούν οι πρώτοι διαιρέτες του n.

Η παρακάτω πρόταση δείχνει ότι το πρόβλημα RSA ανάγεται στο πρόβλημα FACTOR.

Πρόταση 2.1. *Το πρόβλημα RSA έχει πολυωνυμική αναγωγή στο πρόβλημα FACTOR.*

Απόδειξη. Υποθέτουμε ότι έχουμε ένα αλγόριθμο $\mathcal{A}$ ο οποίος επιλύει το πρόβλημα FACTOR. Θα περιγράψουμε ένα αλγόριθμο $\mathcal{B}$ ο οποίος επιλύει το πρόβλημα RSA κάνοντας πολυωνυμικό αριθμό βημάτων και πολυωνυμικό πλήθος κλίσεων του αλγορίθμου $\mathcal{A}$. Έστω, λοιπόν, ότι μας δίνονται φυσικός n (που είναι γινόμενο δύο περιττών πρώτων), φυσικός e τέτοιος ώστε $(e, \phi(n)) = 1$ και ακέραιος b. Θα περιγράψουμε πώς λειτουργεί ο αλγόριθμος $\$cB$. Αρχικά καλεί τον αλγόριθμο $\mathcal{A}$ με είσοδο n και παίρνει ως απάντηση πρώτους p, q τέτοιους ώστε $n = pq$. Στη συνέχεια υπολογίζει το $\phi(n) = (p-1)(q-1)$ και τον αντίστροφο, d, του e modulo $\phi(n)$. Αυτός ο υπολογισμός γίνεται εύκολα με τον επεκτεταμένο Ευκλείδειο αλγόριθμο. Επιστρέφει την τιμή $x = b^d \mod n$. Πραγματικά,

$$x^e \equiv b^{de} \equiv b \pmod{n}.$$

□

Στη συνέχεια δείχνουμε ότι το πρόβλημα αντιστροφής του συστήματος κρυπτογράφης RSA είναι υπολογιστικά ισοδύναμο με το πρόβλημα RSA.

Θεώρημα 2.2. *Το σύστημα κρυπτογράφησης RSA είναι αντιστρέψιμο σε πολυωνυμικό χρόνο αν και μόνο αν το πρόβλημα RSA είναι επιλύσιμο σε πολυωνυμικό χρόνο.*

Απόδειξη. Η απόδειξη είναι προφανής, αν παρατηρήσει κανείς ότι το πρόβλημα αντιστροφής του συστήματος RSA είναι ακριβώς το πρόβλημα RSA. □

Με βάση τα δύο παραπάνω αποτελέσματα βλέπουμε ότι το σύστημα RSA δε μπορεί να είναι ασφαλές αν το πρόβλημα της παραγοντοποίησης είναι υπολογιστικά εύκολο. Άρα είναι σηματνικό να μπορούμε να εκτιμήσουμε πόσο δύσκολο είναι να παραγοντοποιεί κάποιος ακεραίους. Θα μελετήσουμε το πρόβλημα της παραγοντοποίησης ακεραίων σε επόμενο μάθημα. Προς το παρόν θα εξετάσουμε διάφορες άλλες πλευρές της ασφάλειας του RSA.

2.1. **Υπολογισμός του $\phi(n)$ και παραγοντοποίηση.** Στην ενότητα αυτή μελετάμε τη σχέση του προβλήματος υπολογισμού της συνάρτησης ϕ του Euler και του προβλήματος της παραγοντοποίησης.

Πρόταση 2.3. *Έστω φυσικός αριθμός n, ο οποίος είναι γινόμενο δύο περττών πρώτων. Τότε το πρόβλημα του υπολογισμού του $\phi(n)$ είναι υπολογιστικά ισοδύναμο με το πρόβλημα της παραγοντοποίησης του n.*

Απόδειξη. Η μία κατεύθυνση είναι φανερή : Αν κάποιος μπορεί να λύνει το FACTOR, τότε δεδομένου του n υπολογίζει τους πρώτους παράγοντες του, ας πούμε p, q, και υπολογίζει του $\phi(n)$ ως $(p-1)(q-1)$. Στην αντίθετη κατεύθυνση, ας υποθέσουμε ότι έχουμε ένα αλγόριθμο, ο οποίος δεδομένου του n υπολογίζει το $\phi(n)$. Θα περιγράψουμε πώς μπορούμε να υπολογίσουμε την παραγοντοποίηση του n. Γνωρίζουμε ότι $n = pq$ και θέλουμε να υπολογίσουμε τα p, q. Παρατηρούμε ότι

$$\phi(n) = (p-1)(q-1) = pq - (p+q) + 1 = n - s + 1,$$

όπου $s = p + q$. Αρχικά υπολογίζουμε το $\phi(n)$ (έχουμε υποθέσει ότι μπορούμε να το κάνουμε), και στην συνέχεια υπολογίζουμε το

$$s = n + 1 - \phi(n).$$

Παρατηρούμε ότι τα p, q είναι οι ρίζες του τριωνύμου

$$(X-p)(X-q) = X^2 - sX + n.$$

Υπολογίζουμε τις δύο ρίζες του τριωνύμου και βρίσκουμε τους ζητούμενους πρώτους. □

2.2. **Υπολγισμός του d και παραγοντοποίηση.** Φανταστείτε το παρακάτω σενάριο: Μια έμπιστη αρχή δημιουργεί και παραδίνει σε κάθε χρήστη το ζευγάρι των κλειδιών του. Η έμπιστη αυτή αρχή αποφασίζει να επιλέξει τους πρώτους p, q μια φορά. Οι πρώτοι αυτοί, καθώς και το $n = pq$ θα είναι κοινά για όλους. Για κάθε χρήστη θα δημιουργήσει ένα διαφορετικό ζευγάρι εκθετών. Έτσι, τα κλειδιά του χρήστη i θα είναι d_i (το ιδιωτικό) και (n, e_i) (το δημόσιο), όπου φυσικά $e_i d_i \equiv 1 \pmod{\phi(n)}$. Είναι αυτή μια καλή πρακτική; Η παρακάτω πρόταση δείχνει ότι η παραπάνω τακτική καθιστά το σύστημα τελείως ανασφαλές.

Πρόταση 2.4. *Έστω ακέραιος n, ο οποίος είναι γινόμενο δύο περιττών πρώτων. Υπάρχει πιθανοκρατικός αλγόριθμος, ο οποίος δεδομένων του n και ακεραίων d, e τέτοιων ώστε $ed \equiv 1 \pmod{\phi(n)}$ υπολογίζει τους πρώτους παράγοντες του n με πιθανότητα επιτυχίας τουλάχιστο $1 - 2^{-\ell}$ κάνοντας $O(\ell(\log n)^3)$ βήματα.*

Απόδειξη. Ας υποθέσουμε ότι $n = pq$, όπου p, q είναι οι πρώτοι που θέπουμε να υπολογίσουμε. Η σχέση $ed \equiv 1 \pmod{\phi(n)}$ σημαίνει ότι

$$ed - 1 = k(p-1)(q-1),$$

για κάποιο ακέραιο k. Παρατηρήστε ότι το $ed - 1$ είναι άρτιος αριθμός και μπορούμε να τον υπολογίσουμε. Μάλιστα μπορούμε να υπολογίσουμε φυσικούς s, r τέτοιους ώστε $ed - 1 = 2^s r$, r περιττός. Επιλέγουμε τυχαίο ακέραιο $x \in [1, n-1]$. Εάν $(x, n) > 1$, έχουμε υπολογίσει ένα πρώτο παράγοντα του n και έχουμε τελείωσει. Αν $(x, n) = 1$, τότε υπολογίζουμε διαδοχικά τους $x^{2^j r} \mod n$ για $j = 0, \ldots, s$. Ας είναι $j = t$, η πρώτη τιμή του j για την οποία

$$x^{2^t r} \equiv 1 \pmod{n}.$$

Τέτοιο t σίγουρα υπάρχει και στη χειρότερη περίπτωση είναι ίσο με s. Εάν $t = 0$ επιλογή του x είναι αποτυχημένη και επαναλαμβάνουμε τη διαδικασία με διαφορετικό x. Εφόσον ισχύει $t \geq 1$, ας ονομάσουμε $y = x^{2^{t-1} r} \mod n$. Τότε $y \not\equiv 1 \pmod{n}$ και $y^2 \equiv 1 \pmod{n}$. Εάν επιπλέον $y \not\equiv -1 \pmod{n}$ τότε ο μ.κ.δ. $(n, y-1)$ μας δίνει ένα πρώτο παράγοντα του n. Εάν $y \equiv -1 \pmod{n}$ τότε η επιλογή του x είναι αποτυχημένη και επαναλαμβάνουμε με διαφορετικό x.

Ποιά είναι η πιθανότητα μια επιλογή του x να είναι αποτυχημένη; Παρατηρήστε ότι η επιλογή είναι αποτυχημένη αν μια από της παρακάτω ισοτιμίες ικανοποιείται:

$$\begin{aligned} x^r &\equiv 1 \pmod{n} \\ x^{2^j r} &\equiv -1 \pmod{n}, \text{ για κάποιο } 0 \leq j \leq s-1. \end{aligned}$$

Κανείς μετρώντας προσεκτικά μπορεί να δείξει ότι το πολύ οι μισοί ακέραιοι στο διάστημα $[1, n-1]$ είναι δυνατό να ικανοποιούν τουλάχιστο μία από τις παραπάνω ισοτιμίες. Άρα η πιθανότητα να επιλέξουμε «κακό» x είναι το πολύ $1/2$.

Επαναλαμβάνοντας τη διαδικασία ℓ φορές παίρνουμε την πιθανότητα επιτυχίας που αναφέρεται. Το πλήθος των βημάτων για κάθε επιλογή του x δεν είναι περισσότερα από $O((\log n)^3)$. □

Ας δούμε ένα παράδειγμα.

Παράδειγμα 2.5. Έστω $n = 1333$, $e = 11$ και $d = 1104$ και γνωρίζουμε ότι $ed \equiv 1 \pmod{n}$. Θα παραγοντοποιήσουμε το n. Υπολογίζουμε $ed-1 = 2^2 \cdot 2835$. Επιλέγουμε $x = 3$, το οποίο είναι πρώτο προς το n. Υπολογίζουμε

$$3^{2835} \equiv -1 \pmod{n},$$

οπότε η επιλογή $x = 3$ είναι αποτυχημένη. Επιλέγουμε νέο x, έστω $x = 5$. Υπολογίζουμε

$$\begin{aligned} 5^{2835} &\equiv 1117 \pmod{n}, \\ 5^{2 \cdot 2835} &\equiv 1 \pmod{n}. \end{aligned}$$

Τώρα γνωρίζουμε ότι έχουμε επιτύχει! Θέτουμε $y = 1117$, οπότε $y \not\equiv \pm 1 \pmod{n}$ και $y^2 \equiv 1 \pmod{n}$. Για να παραγοντοποιήσουμε το n υπολογίζουμε

$$(n, y-1) = (1333, 1116) = 31.$$

Ο άλλος πρώτος παράγοντας του n είναι ο $n/31 = 1333/31 = 43$.