Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Δημήτριος Μπάκας
Αθανάσιος Ταουσάκος

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

Παρουσίαση:
Δημήτρης Σακαβάλας

23 Νοεμβρίου 2012 (v2)

1 Μερική ανάκτηση πληροφοριών στο RSA

Απλό κείμενο: x
Κρυπτογράφημα: $E(x)$

1. Σπάσιμο: Εξαγωγή του x από το $E(x)$
2. Ανάκτηση μερικής πληροφορίας του x (θα το βρείτε στη βιβλιογραφία και ως Semantic Security)

    - parity bit (last bit)

Για παράδειγμα στο RSA, τουλάχιστον 1 bit διαρρέει, μπορούμε να υπολογίσουμε το σύμβολο Jacobi του απλού κειμένου με τον ακόλουθο τρόπο:
$(\frac{y}{N}) = (\frac{x^e}{p}) \cdot (\frac{x^e}{q}) = (\frac{x}{p})^e \cdot (\frac{x}{q})^e =$ [1] $(\frac{x}{p}) \cdot (\frac{x}{q}) = (\frac{x}{N})$

Δεδομένου ενός κρυπτοκειμένου $y = x^e \pmod N$, μπορεί κανείς να υπολογίσει τη δυαδική ισοτιμία του απλού κειμένου x, δηλαδή το τελευταίο bit του x. Επίσης, μπορεί κανείς να καθορίσει αν ισχύει το $0 < x \leq \frac{N}{2}$ ή το $\frac{N}{2} < x \leq N - 1$.
Ορίζονται δυο συναρτήσεις, η συνάρτηση δυαδικής ισοτιμίας και η συνάρτηση θέσης ως εξής:

$$parity_{N,e}(E_{N,e}(x)) = \begin{cases} 0, & \text{αν } x \text{ άρτιος} \\ 1, & \text{αν } x \text{ περιττός} \end{cases}$$

$$loc_{N,e}(E_{N,e}(x)) = \begin{cases} 0, & \text{αν } x \leq \frac{N}{2} \\ 1, & \text{αν } x > \frac{N}{2} \end{cases}$$

Το να υπολογιστούν τα $loc, parity$ είναι ισοδύναμο με το σπάσιμο του RSA.
Θα δούμε ότι ο υπολογισμός του parity είναι πολυωνυμικά ισοδύναμος με τον υπολογισμό του $loc_{N,e}$. Με το $E_{N,e}(x)$ ορίζουμε την κρυπτογράφηση του x σε $y = E_{N,e}(x) = x^e \pmod N$ και με $D_{N,e}(y) = x$ την αποκρυπτογράφηση.
Ξέρουμε ότι η $E_{N,e}$ είναι ομοιομορφική ως προς τον πολλαπλασιασμό δηλαδή:
$E_{N,e}(x_1) \cdot E_{N,e}(x_2) = E_{N,e}(x_1 \cdot x_2)$
Αποδεικνύεται εύκολα ότι:

- $loc_{N,e}(y) = parity_{N,e}(y \cdot E_{N,e}(2) \pmod N) = parity_{N,e}(E_{N,e}(2x))$
- $parity_{N,e}(y) = loc_{N,e}(y \cdot E_{N,e}(2^{-1}) \pmod N) = loc_{N,e}(E_{N,e}(2^{-1} \cdot x))$

Ο αλγόριθμος για την εύρεση του απλού κειμένου $x = D_{N,e}(y)$ βασίζεται στην τεχνική της δυαδικής αναζήτησης.

[1] γιατί το e είναι περιττό αφού $gcd(e, \phi(N)) = 1, \phi(N)$ άρτιος

$y_0 = loc_{N,e}(x) = y$
$y_i = loc_{N,e}(y_{i-1} \cdot E_{N,e}(2)) = loc_{N,e}(y \cdot (E_{N,e}(2))^i) = loc_{N,e}(E_{N,e}(x \cdot 2^i))$
όπου $0 \leq i \leq \lfloor log_2 N \rfloor$ και $y_0 = E_{N,e}(x) = y$
Παρατηρούμε ότι:
Για $y_0 = 0 : loc_{N,e}(E_{N,e}(x)) = 0 \iff x \in [0, \frac{N}{2})$

Για $y_1 = loc_{N,e}(E_{N,e}(2x)) = 0 \iff x \in [0, \frac{N}{4}) \cup [\frac{N}{2}, \frac{3N}{4})$

Για $y_2 = loc_{N,e}(E_{N,e}(4x)) = 0 \iff x \in [0, \frac{N}{8}) \cup [\frac{N}{4}, \frac{3N}{8}) \cup [\frac{N}{2}, \frac{5N}{8}) \cup [\frac{3N}{4}, \frac{7N}{8})$
κ.ο.κ.

Παρατήρηση: Αφού υπάρχει αποδοτικός αλγόριθμος για το parity που είναι ισοδύναμος με το location, τότε υπάρχει αποδοτικός αλγόριθμος για το σπάσιμο του RSA ισοδύναμος και με τα 2.

Πιθανοτική Κρυπτογράφηση
Αν σκεφτούμε πως η Alice θέλει να στείλει 1 bit στον Bob:

$$b \in \{0, 1\}$$

$$y = b^e \pmod N = \begin{cases} 0, & \text{αν b=0} \\ 1, & \text{αν b=1} \end{cases}$$

Επειδή από το παραπάνω παράδειγμα βλέπουμε πως δεν λειτουργεί η απλή αποστολή ενός 0 ή 1,η Alice θα πρέπει διαλέξει τυχαία κάποιο $x < \frac{N}{2} - 1$, $y = (2x + b)^e$.
Ο Bob αποκρυπτογραφεί και παίρνει το τελευταίο bit. $D(y) = (2x+b) \pmod N$.

Άσκηση
Υποθέτουμε πως μία εταιρεία (τα παλιά χρόνια) είχε ζητήσει από τους υπαλλήλους της να επιλέγουν δημόσια κλειδιά $(N, 3)$ ώστε η κρυπτογράφηση να είναι γρήγορη και να μην σπαταλούνται οι διαθέσιμοι υπολογιστικοί εταιρικοί πόροι. Οι υπάλληλοι λοιπόν με τον περιορισμό το $gcd(3, \phi(n)) = 1$ επιλέγουν με τυχαίο τρόπο p, q ώστε να σχηματίσουν τα δημόσια κλειδιά τους. Η Alice, που είναι υπάλληλος της εταιρείας, επιθυμεί να στείλει στους τρεις συνα- δέλφους της Bob, Charlie και Diane ένα ιδιαίτερα σημαντικό μήνυμα, έστω m. Η Eve, που δουλεύει σε μια ανταγωνιστική εταιρεία, καταφέρνει και υποκλέπτει τα κρυπτομήνυμα C_i με $i \in \{1, 2, 3\}$. Θα μπορέσει η Eve να αποκρυπτογραφήσει το μήνυμα;

Έστω τα δημόσια κλειδιά των Bob, Charlie και Diane $A_1 = (N_1, 3), A_2 = (N_2, 3), A_3 = (N_3, 3)$.

Η Eve σχηματίζει το σύστημα
$c_1 = m^e \pmod{N_1}$

$c_2 = m^e \pmod{N_2}$
$c_3 = m^e \pmod{N_3}$

ή αλλιώς
$m^3 = c_1 \pmod{N_1}$
$m^3 = c_2 \pmod{N_2}$
$m^3 = c_3 \pmod{N_3}$

Αφού διαλέξαμε τυχαίους πρώτους αριθμούς υπάρχει μεγάλη πιθανότητα να είναι και πρώτοι μεταξύ τους. Άρα, απο το Κινέζικο Θεώρημα Υπολοίπων η Eve υπολογίζει:

$$u = m^3 \pmod{N_1 N_2 N_3}$$

Κι επειδή γνωρίζει πως $m < N_i, \forall i \in \{1, 2, 3\}$ τελικά υπολογίζει

$$m = \sqrt[3]{x}$$

.

Βιβλιογραφία

Zac12 : Σημειώσεις Ζάχου, ΕΜΠ, 2012.

Sti06 : D. Stinson: Cryptography: Theory and Practice, 3rd edition, CRC Press, 2005.