Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

Επιμέλεια σημειώσεων:
Κωνσταντίνος Μάστακας
Στράτος Παλαιολόγος

Παρουσίαση:
Δημήτρης Σακαβάλας
Γιώργος Ζηρδέλης

26 Νοεμβρίου 2012

1 Συναρτήσεις μονής κατεύθυνσης

Υποψήφιες συναρτήσεις: Έστω p, q πρώτοι τότε $f_{\text{mult}}(p, q) = pq$

$f_{\text{RSA}}(x, e, p, q) = (x^e \pmod{pq}, pq, e)$

Άλλη υποψήφια μπορεί να είναι η $f_{\text{exp}}(g, x) = (g, g^x)$

Αν έχω το g και το x υπολογίζω εύκολα το g^x. Αντίστροφα, αν έχω το g^x και το g είναι δύσκολο να υπολογίσω το $x = \log_g x$.

Το $\mathbb{F}_q^*$ είναι σώμα αν και μόνο αν $q = p^k, p$ πρώτος

2 Διακριτός Λογάριθμος

Έστω $(G, *)$ πεπερασμένη κυκλική ομάδα τάξης n και έστω ένας γεννήτορας της ομάδας $g(< g >= G), b \in G$ τότε υπάρχει μοναδικό $x \in \langle 0, 1, \ldots, n-1\rangle$ τέτοιο ώστε $g^x = b$ ισοδύναμα $\log_g b = x$.

Πρόβλημα του Διακριτού Λογαρίθμου (DLP) Δίνεται ένας πρώτος p και ένας γεννήτορας g του $\mathbb{Z}_p^*$ και $b \in \mathbb{Z}_p^*$. Να βρεθεί $x \in \{0, 1, \ldots, p-2\}$ τέτοιο ώστε $g^x = b \pmod{p}$.

Πρόταση 1 Έστω πρώτος p και ένας γεννήτορας g του $\mathbb{Z}_p^*$ τότε ισχύει ότι $g^n = g^m \pmod{p}$ αν και μόνο αν $n = m \pmod{p-1}$.

Απόδειξη
"$\Leftarrow$"

Αν $(g, p) = 1$ τότε υπάρχει ο αντίστροφος του g δηλ. ο (g^{-1}). Έχουμε ότι $n = m \pmod{p-1} \Rightarrow n - m = k(p-1)$ και από το θεώρημα του Fermat έχουμε $g^{(p-1)} = 1 \pmod{p} \Rightarrow (g^{p-1})^k = 1 \pmod{p} \Rightarrow g^{n-m} = 1 \pmod{p} \Rightarrow g^n g^{-m} = 1 \pmod{p} \Rightarrow g^n = g^m \pmod{p}$.
"$\Rightarrow$"

Για κάθε $r \in \mathbb{N}$ τέτοιο ώστε $g^r = 1 \pmod{p} \Rightarrow p - 1 | r$ οπότε $g^n = g^m \pmod{p} \Rightarrow g^{n-m} = 1 \pmod{p} \Rightarrow n - m = k(p-1) \Rightarrow n = m \pmod{p-1}$.

Θεώρημα: Έστω g, g' γεννήτορες της $\mathbb{Z}_p^*$ και $b \in \mathbb{Z}_p^*$ τότε ισχύει ότι
$\log_{g'} b = \log_g b \cdot (\log_g g')^{-1} \pmod{p}$.

Απόδειξη Έστω $x = \log_g b, y = \log_{g'} b$ και $z = \log_g g'$ τότε $g^x = b = g'^y = (g^z)^y \pmod{p} \Rightarrow g^x = g^{zy} \pmod{p} \Rightarrow x = zy \pmod{p-1} \Rightarrow y = xz^{-1} \pmod{p-1}$.

Πρόβλημα LSB Ασφάλεια τελευταίου bit. Δεδομένου δηλαδή του $g^x = y \pmod{p}$ να υπολογίσω το τελευταίο bit του x (ή αλλιώς αν το x είναι άρτιος ή περιττός).

Γνωρίζω ότι $g^{p-1} = 1 \pmod{p} \Rightarrow g^{(\frac{p-1}{2})^2} = 1 \pmod{p} \Rightarrow g^{\frac{p-1}{2}} = 1 \pmod{p}$ ή $g^{\frac{p-1}{2}} = -1 \pmod{p}$. Επίσης, $\text{ord}_p(g) = p-1$ οπότε $g^{\frac{p-1}{2}} = -1 \pmod{p}$. Χρησιμοποιώντας αυτήν την παρατήρηση έχουμε ότι $y = g^x \pmod{p} \Rightarrow y^{\frac{p-1}{2}} = g^{x\frac{p-1}{2}} =$

$\left(g^{\frac{p-1}{2}}\right)^x = (-1)^x \pmod p$. Επομένως

$$y^{\frac{p-1}{2}} = \begin{cases} 1, & x \text{ άρτιος} \\ -1, & x \text{ περιττός} \end{cases}$$

$1, x$ άρτιος ή $-1, x$ περιττός.

Από αυτό το πρόβλημα (DLP) ξεκίνησε η ιδέα των κρυπτοσυστημάτων δημοσίου κλειδιού.

Ανταλλαγή κλειδιού Diffie - Hellman

1. Δημοσίευση $p, g, < g >= \mathbb{Z}_p^*$,
2. - Η Alice επιλέγει τυχαίο $x \in \mathbb{Z}$ και στέλνει $g^x \pmod p$
   - Ο Bob επιλέγει τυχαίο $y \in \mathbb{Z}$ και στέλνει $g^y \pmod p$
3. Η Alice υπολογίζει $K = (g^y)^x = g^{xy} \pmod p$ και ο Bob υπολογίζει $K = (g^x)^y = g^{xy} \pmod p$.

Με αυτόν τον τρόπο ανταλλάσουν κοινό κλειδί χωρίς να δημοσιεύσουν τα x και τα y, αλλά δημοσιεύοντας τα g^x και g^y. Για να σπάσει αυτό το σύστημα δε χρειάζεται ακριβώς να λυθεί το DLP, αλλά ένα άλλο πρόβλημα το DHP(Diffie - Hellman), όπου DHP$\leq_P$DLP. *DHP* Δίνεται $p, g, < g >= \mathbb{Z}_p^*$, $a = g^x \pmod p, b = g^y \pmod p$, βρές $c = g^{xy} \pmod p$.

Το κρυπτοσύστημα ElGamal

Το κρυπτοσύστημα δημοσίου κλειδιού ElGamal προτάθηκε στο *Crypto '84* από τον Taher ElGamal. Έστω ότι ο Bob θέλει να στείλει ένα μήνυμα στην Alice.

Η Alice διαλέγει ένα πρώτο p, όπου ο $p-1$ (η τάξη) έχει τουλάχιστον ένα μεγάλο παράγοντα, ένα γεννήτορα g της $\mathbb{Z}_p^*$ και τα δημοσιοποιεί.

1. Η Alice διαλέγει τυχαίο $a \in \{1, 2, \ldots, p-1\}$ και υπολογίζει $A = g^a \pmod p$. Το a είναι το μυστικό κλειδί της Alice ενώ το A το δημόσιο κλειδί της.
2. Ο Bob διαλέγει $m \in \{1, 2, \ldots, p-1\}$ και τυχαίο $k \in \{2, 3, \ldots, p-1\}$.
3. (κρυπτογράφηση) Ο Bob υπολογίζει $r = g^k \pmod p$ και $c = mA^k \pmod p$ και στέλνει το ζευγάρι (r, c) στην Alice (έχουμε 2-to-1 message expansion).
4. (απόκρυπτογράφηση) Η Alice υπολογίζει πρώτα: $r^a = (g^k)^a = g^{ka} \pmod p$ και $(g^{ka})^{-1}$.

   Μετά, για το μήνυμα m υπολογίζει: $(g^{ka})^{-1} \cdot c = (g^{ka})^{-1}(mA^k) = (g^{a^k})^{-1} \cdot (m \cdot (g^a)^k) = (g^{ak})^{-1} \cdot m \cdot g^{ak} = m \pmod p$.

Επειδή το r είναι τυχαίο η κρυπτογράφηση είναι πιθανοτική.

Επίθεση όταν χρησιμοποιείται το ίδιο r

Έχουμε m_1, m_2 (δύο plaintexts) και (r, c_1), (r, c_2) τα αντίστοιχα κρυπτοκείμενα. Επίσης υποθέτουμε οτι η Eve γνωρίζει το m_1.

Οπότε η Eve γνωρίζοντας τα r, c_1, c_2, m_1, υπολογίζει το m_2 όπως φαίνεται παρακάτω:

$$\left.\begin{array}{ll} c_1 = m_1 A^k & (\text{mod } p) \\ c_2 = m_2 A^k & (\text{mod } p) \end{array}\right\} \Rightarrow \left.\begin{array}{ll} c_2 = m_2 g^{ka} & (\text{mod } p) \\ c_1 = m_1 g^{ka} & (\text{mod } p) \end{array}\right\} \Rightarrow \begin{cases} c_2 (g^{ka})^{-1} = m_2 & (\text{mod } p) \\ c_1^{-1} m_1 = (g^{ka})^{-1} & (\text{mod } p) \end{cases}$$

Άρα $m_2 = c_2 (c_1)^{-1} m_1$ και έτσι η Eve υπολογίζει το m_2.

Βιβλιογραφία

Zac12 : Σημειώσεις Ζάχου, ΕΜΠ, 2012.

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