Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Κάβουρας Λουκάς
Παπαδιάς Σεραφείμ

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

11 Ιανουαρίου 2013

1 Ανταλλαγή Κλειδιού Diffie-Hellman

Υποθέτουμε τον πρώτο p και g γεννήτορα του συνόλου $\mathbb{Z}_p^*$.Η Α (Alice) επιλέγει $x_A \in \mathbb{Z}_{p-1}$ και στέλνει το g^{x_A} στον Β (Bob).Και ο Bob με τη σειρά του επιλέγει $x \in \mathbb{Z}_{p-1}$ και στέλνει το g^{x_B} στην Α. Και μετά ο καθένας υπολογίζει το κλειδί από αυτό που του ήρθε υψώνοντας το στο δικό του εκθέτη $k = g^{x_A x_B} \bmod p$.
Για να υπολογίσει κάποιος τρίτος το $g^{x_A x_B}$ πρέπει να λύσει το πρόβλημα Diffie-Hellman .
DHP(Diffie-Hellman Problem): Δίνονται g^{x_1} , g^{x_2} και πρέπει να υπολογιστεί το $g^{x_1 x_2}$.Ισχύει DHP $\leq^P$ DLP , όπου DLP ο διακριτός λογάριθμος.

2 Σχήματα αναγνώρισης(ταυτοποίησης)/Identification (user authentication)

- **passwords :** encrypted (συνήθως) , replay problem
- **αποδείξης γνώσης (proofs of knowledge) :** κάθε μέρα είναι διαφορετικές με χρήση κάποιας τυχαιότητας.
- **Με χρήση συμμετρικής κρυπτογραφίας :** Έστω **κοινό κλειδί** k και χρειαζόμαστε μία συνάρτηση e_k.Η Α αιτείται στον Β, και ο Β επιλέγει και στέλνει x στην Α.Η Α υπολογίζει $y = e_k(x)$ και το στέλνει στον Β.Ο Β για να ταυτοποιήσει την Α, υπολογίζει το $e_k(x)$ και ελέγχει αν $y = e_k(x)$ (το $e_k(x)$ υπολογισμένο από τον Β).
  Έτσι, πιθανόν μετά από κάμποσες επαναλήψεις ο αντίπαλος έχει πληροφορία για κείμενα και κρυπτοκείμενα, άρα και για το κλειδί.
- **Με ιδέα συστήματος δημοσίου κλειδιού :** Η Α αιτείται στον Β, και ο Β επιλέγει και στένλνει $y = enc_{P_A}(x)$ στην Α.Η Α υπολογίζει $z = dec_{S_A}(y)$ και το στέλνει στον Β.Ο Β για να ταυτοποιήσει την Α, ελέγχει αν $x = z$ για να είναι αποδεκτό.
  Έτσι και εδώ, έχουμε το ίδιο πρόβλημα με προηγουμένως. Υπάρχουν καλύτερες τεχνικές identification που βασίζονται στην τυχαιότητα.

3 Σχήμα Αναγνώρισης Schorr

Αρχικοποίηση: p , q primes και $q|(p-1)$, τυπικές τιμές $p \approx 2^1024$, $q \approx 2^{160}$, γεννήτορας $g \in \mathbb{Z}_p^*$ αλλά είναι τάξης q , $g^q \equiv 1(\bmod p)$.

Ορίζεται η παράμετρος t : $2^t < q$ και $t = 40$ (συνήθως).Η trusted authority παρέχει sig_T, ver_T, $C(A) =< ID(A), v, s >$, $sig_T(ID(A), v)$.Και ο Α δημοσιεύει $< ID(A), v, C(A) >$, $v = g^{-a}$ όπου $a \in \mathbb{Z}_q$ ειναι ιδιωτικός μυστικός εκθέτης η

μυστικό κλειδί που είναι γνωστός μόνο στην Α (δεν το στέλνει ούτε στην έμπιστη αρχή).

3.1 Πρωτόκολλο Schorr

1. Η Α επιλέγει τυχαία $k \in \mathbb{Z}_q^*$ και στέλνει στον Β $\gamma = g^k \bmod p$.
2. Ο Β επαληθεύει $< ID(A), v, C(A) >$ και sig_T επιλέγει τυχαία $r \in [0, .., 2^t]$ και στέλνει το r στην Α.
3. Ο Α στέλνει το $y = k + a \cdot r \bmod q$ στον Β.
4. Ο Β ελέγχει αν $\gamma \equiv g^y \cdot v^r (\text{mod} p)$.

3.2 Τυποποίηση

1. commitment
2. challenge
3. response
4. response

Commpletness: Αν παίζουν "τίμια" η αναγνώριση επιτυγχάνει.
Soundness: Αν όχι τότε αποτυγχάνει η αναγνώριση ή αποτυγχάνει με μεγάλη πιθανότητα.

1. $g^y \cdot v^r \equiv g^{y-a \cdot r} \equiv g^k \equiv \gamma (\text{mod} p)$.Άρα έχουμε ορθότητα.
2. Soundness:(Τι θα μπορούσε να κάνει η Όλγα(Ο) για να προσποηθεί ότι είναι η Α στον Β?) .Συμμετέχει στην επιλογή του $k \in \mathbb{Z}_q$ και στέλνει $\gamma = g^y \cdot v^r \bmod p$ με πιθανότητα επιτυχίας $\frac{1}{2^t}$ μόνο.Αν μπορεί για διαφορετικά r_1, r_2 να υπολογίζει y_1, y_2 τέτοια ώστε να επαληθεύονται τότε θα ισχύει το εξής: $g^{y_1} \cdot v^{r_1} \equiv \gamma \equiv g^{y_2} \cdot v^{r_2} \Leftrightarrow y_1 - a \cdot r_1 \equiv y_2 - a \cdot r_2 (\text{mod} q) \Leftrightarrow a \equiv (y_2 - y_1) \cdot (y_2 - y_1)^{-1} (\text{mod} q)$, πρέπει $(r_2 - r_1, q) = 1$.Αυτό ισχύει γιατί $-q < r_2 - r_1 < q$ άρα $r_2 - r_1$ πρώτος με το q.

Άρα υπολογιστικά αν μπρούσε να το κάνει αυτό θα μπορούσε να υπολογίσει διακριτό λογάριθμο.

Βιβλιογραφία

Zac12 : Σημειώσεις Ζάχου, ΕΜΠ, 2012.

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