Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Ελένη Πύλια
Κατερίνα Σωτηράκη

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

14 Δεκεμβρίου 2012

1 Ψηφιακές Υπογραφές

1. Authentication (γνησιότητα):το μήνυμα προέρχεται από το σωστό αποστολέα.
2. Non-repudiation (μη αποκήρυξη): δεν μπορεί κάποιος να "αποκηρύξει" τη δική του υπογραφή.
3. Data Integrity (ακεραιότητα δεδομένων): συνήθως προκύπτει σαν παράπλευρο αποτέλεσμα.
4. Υπολογιστική ευκολία της δημιουργίας υπογραφής (για το νόμιμο αποστολέα μόνο) και επαλήθευσης (για όλους).

Χρήση κρυπτογραφίας δημοσίου κλειδιού:

Ιδιωτικό κλειδί $\Rightarrow$ δημιουργία υπογραφής
Δημόσιο κλειδί $\Rightarrow$ επαλήθευση υπογραφής

Σχήμα υπογραφής:

- Παραγωγή κλειδιών: Συνήθως όπως στο "αντίστοιχο" σχήμα κρυπτογράφησης/αποκρυπτογράφησης.
- (Αλγόριθμος/Συνάρτηση) $sig : M \times K \to S$, όπου M είναι τα μηνύματα, K είναι τα κλειδιά και S είναι οι υπογραφές.
  Αν το κλειδί είναι "φιξαρισμένο": $sig_{s_A} : M \to S$, όπου s_A είναι το ιδιωτικό κλειδί του χρήστη A.
- (Αλγόριθμος/Συνάρτηση) $ver_{p_A} : M \times S \to \{True, False\}$, όπου p_A είναι το δημόσιο κλειδί του χρήστη A.

RSA signature

Κλειδιά: $s_A = d, p_A = (e, d)$ όπου $(e, d) \in \mathbb{Z}_n$ και $ed \equiv 1 \bmod \phi(n)$
$sig : \forall m \in M : s = sig_{s_A}(m) = m^d \underline{\text{mod}} n$
$ver : ver_{p_A}(m, s) = TRUE \Leftrightarrow m = s^e \underline{\text{mod}} n$

Αν $m = s^e + in$, τότε $ver_{p_A}(m, s) = TRUE$, δηλαδή, $\forall m \in M : m = s^e + in \Rightarrow ver_{p_A}(m, s) = TRUE$

Στην περίπτωση που τα μηνύματα μπορούν να έχουν "οποιαδήποτε" μορφή, χρησιμοποιούμε μια συνάρτηση πλεονάζουσας πληροφορίας (η οποία πρέπει να είναι αντιστρεπτή, 1 προς 1 και υπολογιστικά εύκολη), π.χ. απαιτούμε μετά από κάθε 4 bits να υπάρχει το 101.

Δε θα πρέπει να ισχύει $f(m_1m_2) = f(m_1)f(m_2)$, όπου f η συνάρτηση πλεονάζουσας πληροφορίας.
Αν ισχύει, τότε $s_1s_2 = sig(f(m_1))sig(f(m_2)) = f(m_1)^d f(m_2)^d = (f(m_1)f(m_2))^d = f(m_1m_2)^d = sig(f(m_1m_2))$. Άρα, από τα $sig(f(m_1)), sig(f(m_2))$ μπορούμε να βρούμε το $sig(f(m_1m_2))$.
Γενικότερα, δεν πρέπει να ισχύει $f(m_1)f(m_2) = f(m_3)$ για κάποιο μήνυμα m_3.

Encryption and Signing
Έστω ότι ο Α στέλνει στον Β.

1. Encrypt-then-sign
    - Ο Β λαμβάνει: $(enc_{p_B}(m), sig_{s_A}(enc_{p_B}(m)))$, επαληθεύει και αποκρυπτογραφεί.
    - Πρόβλημα:Έστω ότι ο Ο βρίσκεται ανάμεσα στους Α,Β.Ο Ο παίρνει το παραπάνω ζευγάρι, βάζει τη δικιά του υπογραφή και στέλνει,σα δικό του, αυτό που θα έστελνε ο Α.Στέλνει,δηλαδή, $(enc_{p_B}(m), sig_{s_O}(enc_{p_B}(m)))$. Σε αυτή την περίπτωση, αν ο Β απαντήσει στον Ο κάτι σχετικό, τότε ο Ο θα μπορεί να ανακτήσει κάποιες πληροφορίες για το m.
2. Sign-then-encrypt
    - Ο Β λαμβάνει: $enc_{p_B}(m, sig_{s_A}(m))$, αποκρυπτογραφεί και έχει: $(m, sig_{s_A}(m))$.
    - Πρόβλημα:Ο Β έχει την υπογραφή του Α και μπορεί να στείλει το m αλλού (σα να το στέλνει ο Α).

ElGamal Signature Scheme

- Κλειδιά:πρώτος p,γεννήτορας g,$\beta = g^\alpha$,$\alpha \in [2, ..., p-2]$
  public:(p,g,Β)
  secret:α
- Υπογραφή:Επιλέγεται τυχαίο $\kappa \in \mathbb{Z}^*_{p-1}$.
  $\gamma = g^\kappa \underline{mod} p$
  $\delta = (m - \alpha \cdot \gamma) \cdot \kappa^{-1} \underline{mod}(p-1)$
  $sig(m, \kappa) = (\gamma, \delta)$
  $ver(m, \gamma, \delta) = TRUE \Leftrightarrow \beta^\gamma \cdot \gamma^\delta \equiv g^m \bmod p$(σχέση (1))

Σημείωση:Το σχήμα αυτό είναι μη ντετερμινιστικό, δηλαδή υπάρχουν πολλές έγκυρες υπογραφές για το m.

Σενάρια Πλαστογράφησης:

1. Επιλέγω m και προσπαθώ να βρώ γ,δ ώστε να ικανοποιείται η (1).
   - Επιλέγω και γ, ψάχνω δ τέτοιο ώστε να ικανοποιείται η (1):θα πρέπει $\gamma^{\delta} \equiv g^{m} \cdot \beta^{-\gamma} \bmod p$ (DLP).
   - Επιλέγω και δ,ψάχνω γ τέτοιο ώστε να ικανοποιείται η (1). Το πρόβλημα επίλυσης της (1) ως προς γ είναι ανοιχτό.
2. Επιλέγω γ και δ,ψάχνω m:DLP
3. Επιλέγω γ, δ, m ταυτόχρονα.
   Ορίζουμε: $\gamma = g^{i} \cdot \beta^{j}$,0 $\leq$i,j$\leq p-2$,$gcd(j, p-1) = 1$
   $\delta = -\gamma \cdot j^{-1} \underline{mod}(p-1)$
   $m = -\gamma \cdot i \cdot j^{-1} \underline{mod}(p-1)$