Κρυπτογραφία

Εργαστηριακό μάθημα 7
(Αλγόριθμοι Δημοσίου Κλειδιού)
α) El Gamal
β) Diffie-Hellman αλγόριθμος για την ανταλλαγή συμμετρικού κλειδιού κρυπτογράφησης

El Gamal Αλγόριθμος

- Παράμετροι συστήματος: Ακέραιοι g,p
- Ο p είναι ένας πολύ μεγάλος πρώτος και ο g ένα πρωταρχικό στοιχείο (στοιχείο – γεννήτορας) του Z_p^*.

(δηλαδή: $g^k \neq 1 \pmod p$ για όλα τα k μικρότερα του p-1)

(με Z_p^* συμβολίζουμε το σύνολο όλων των ακεραίων 1,2,…,p-1. Ονομάζεται πεπερασμένη ομάδα – όλες οι πράξεις σε μία ομάδα γίνονται modulo p).

Τα p,g επιλέγονται τυχαία από έναν χρήστη Α.

- Ο Α επιλέγει ιδιωτικό κλειδί a: $1 < a < p - 1$
- Υπολογισμός του $y = g^a \bmod p$.
- Το Δημόσιο Κλειδί του Α είναι η τριπλέτα (p, g, y). Το ιδιωτικό του κλειδί είναι το a.

Ένα σημαντικό σχόλιο για τους γεννήτορες

- Αν ισχύει $g^k = 1 \bmod p$ για κάποιον ακέραιο αριθμό $1<k<p-1$, τότε ο αριθμός k υποχρεωτικά διαιρεί το p-1.
- Άρα, αν θέλουμε να ελέγξουμε αν ένας αριθμός g είναι γεννήτορας mod p, δεν χρειάζεται να τον υψώσουμε σε όλες τις δυνάμεις 1,2,..,p-1!! Αρκεί να τον υψώσουμε στους διαιρέτες του p-1.

Κρυπτογράφηση El Gamal

Αν ο Β θέλει να στείλει ένα μήνυμα m στον Α, τότε:

- Ο Β παράγει τυχαίο ακέραιο k, 1< k < p-1.
- Ο Β στέλνει το $\gamma = g^k \pmod p$ και το
  $\delta = my^k \pmod p$ στον Α.
- Αποκρυπτογράφηση: Ο Α χρησιμοποιεί τη γνώση του μυστικού κλειδιού a για τον υπολογισμό του m.

Αποκρυπτογράφηση El Gamal

- Ο δέκτης Α υπολογίζει το γ^{-a}
  (μια που γνωρίζει το ιδιωτικό του κλειδί a)
- Ο Α ανακτά το μήνυμα m με τον υπολογισμό
  $(\gamma^{-a})\delta \bmod p$.
- **Επαλήθευση: $(\gamma^{-a})\delta \equiv \gamma^{-a}\delta \equiv g^{-ak}\, my^{k} \equiv g^{-ak}\, mg^{ak} \equiv m \bmod p.$**
- **Με άλλα λόγια: το κρυπτόγραμμα είναι το ζεύγος (γ,δ) και η ανάκτηση του αρχικού μηνύματος γίνεται με την πράξη δ/γ^{a}**

Χαρακτηριστικά του αλγορίθμου El Gamal

- Το κρυπτόγραμμα είναι δύο φορές πιο μεγάλο από το μήνυμα (βασικό του μειονέκτημα έναντι του RSA)
- Η ασφάλειά του στηρίζεται στη δυσκολία επίλυσης των προβλημάτων DLP (Discrete Logarithm Problem) - Για δοθέν $h=g^a \bmod p$, υπολογισμός του a είναι αδύνατος ακόμα κι αν ξέρουμε τα g,p,h όταν αυτά είναι τεράστιοι αριθμοί

Παράδειγμα κρυπτογράφησης El Gamal

Παράμετροι δημοσίου κλειδιού:

p = 11

g = 6 (μπορούμε να επιβεβαιώσουμε με δοκιμές ότι πράγματι το g είναι γεννήτορας του Z_{11}^*.)

(προσέξτε ότι ο αριθμός 4 δεν είναι γεννήτορας του Z_{11}^*!! Μπορείτε να δείτε γιατί?)

Μυστικό κλειδί του χρήστη: a = 2

Υπολογισμός του: $y \equiv g^a \bmod p \Rightarrow y = 6^2 = 36 = 3 \bmod 11$

Τα p,g,y δημοσιοποιούνται. Το a κρατείται μυστικό.

Παράδειγμα κρυπτογράφησης El Gamal (συνέχεια)

Έστω ότι στον προηγούμενο χρήστη θέλουμε να στείλουμε το μήνυμα m=9.

1. Επιλογή τυχαίου αριθμού k (έστω $k = 2$)
2. Υπολογισμός των
   1. $\gamma \equiv g^k \bmod p \equiv 36 = 3 \bmod 11$
   2. $\delta = y^k m \bmod p \equiv 9 \cdot 9 = 81 \bmod 11 = 4 \bmod 11$
3. Κρυπτόγραμμα είναι το ζευγάρι (γ,δ)=(3,4)

ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ

Το μήνυμα m ανακτάται από τη σχέση: $\delta/\gamma^a \bmod 11 \equiv 4/3^2 \bmod 11$

Έχουμε $3^2 \equiv 9 \bmod 11$

Άρα το μήνυμα m είναι το $4 \cdot 9^{-1} \bmod 11$

Ο αντίστροφος του 9 mod 11 είναι προφανώς ο 5 (μπορεί να υπολογιστεί με δοκιμές)

Συνεπώς το αποκρυπτογραφημένο μήνυμα είναι $4 \cdot 5 \bmod 11 \equiv 20 \equiv \mathbf{9} \bmod 11$

Κρυπτογράφηση El Gamal – Παράδειγμα 2

- Πρώτος $p = 2357$ Πρωταρχικό στοιχείο $g = 2$
- Ιδιωτικό κλειδί: $a = 1751$
- $y = 2^{1751} (\text{mod } 2357) = 1185$
- *Μήνυμα* $m = 2035$
- Έστω τυχαίος ακέραιος $k = 1520$ που παράγει ο αποστολέας.

  Τότε, κάνει τους εξής υπολογισμούς:
  - $\gamma = g^k = 2^{1520} (\text{mod } 2357) = 1430$
  - $\delta = my^k = 2035 \cdot 1185^{1520} (\text{mod } 2357) = 697$
  - Οι πράξεις και εδώ μπορούν να γίνουν με την τεχνική Square-And-Multiply (βλέπε RSA)
- Συνεπώς, μεταδίδεται το ζεύγος (1430, 697) από τον Β στον Α

Κρυπτογράφηση El Gamal – Παράδειγμα 2 (συνέχεια)

Για την αποκρυπτογράφηση:

$$\gamma^{-a} \equiv 1430^{605} \bmod 2357 = 872$$

(μια που $\gamma^{-a} \equiv \gamma^{p-1-a}$, αφού $\gamma^{p-1} \equiv 1 \bmod p$).

Εύρεση *m*: $872 \cdot 697 \bmod 2357 = 2035$

Υλοποιήσεις σε MATLAB κρυπτογραφικών αλγορίθμων

- ## Αλγόριθμος El Gamal

  http://islab.oregonstate.edu/koc/ece575/02Project/Sin+Cha/

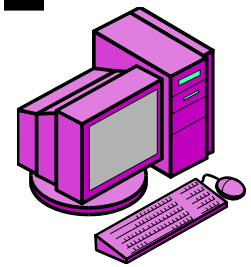
Εκτελείται ως εξής:

1. Πρώτα εκτελούμε την pub_key_gen, η οποία παράγει τα δημόσια κλειδιά p, Alpha, Betaa (και υπολογίζει και το ιδιωτικό κλειδί που το κρατάει μυστικό). Η μεταβλητή Alpha αντιστοιχεί στον γεννήτορα g, ενώ η Betaa στο y.
2. Μετά, τρέχουμε τη συνάρτηση encrypt, όπου μας ζητά να δώσουμε ένα κείμενο (με μικρά γράμματα, χωρίς κενά και χωρίς σημεία στίξης). Η συνάρτηση αυτή υπολογίζει τα δ,γ που τα αντιστοιχεί στις μεταβλητές y1, y2 αντίστοιχα.
3. Τέλος τρέχουμε τη συνάρτηση decrypt με ορίσματα τα y1,y2 (δηλαδή γράφουμε decrypt(y1,y2)). Λογικά, θα πάρουμε το αρχικό μήνυμα

Κρυπτογράφηση με συμμετρικό ή με Δημόσιο κλειδί?

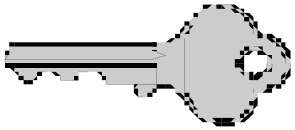
- Οι σύγχρονοι αλγόριθμοι συμμετρικού κλειδιού (block ciphers/stream ciphers) είναι πιο γρήγοροι από τους αλγορίθμους Δημοσίου κλειδιού και χρησιμοποιούνται περισσότερο.
  - Μειονέκτημα: πρέπει οι δύο συνομιλούντες να ανταλλάξουν το κοινό κλειδί κρυπτογράφησης πριν ξεκινήσει η επικοινωνία (*π.χ. στον Vigenere αλγόριθμο για να μπορεί ο παραλήπτης να αποκρυπτογραφήσει πρέπει να ξέρει τη φράση-κλειδί*). Πώς μπορεί να γίνει αυτό, τη στιγμή που δεν υπάρχει ασφαλές κανάλι επικοινωνίας?
- Η ανταλλαγή του συμμετρικού κλειδιού κρυπτογράφησης γίνεται με κάποιον αλγόριθμο Δημοσίου κλειδιού. (όπου πραγματικά, σε αλγορίθμους Δημοσίου Κλειδιού, δεν απαιτείται καμία εκ των προτέρων ανταλλαγή πληροφορίας των δύο συνδιαλεγομένων).
- Συνεπώς, οι δύο μέθοδοι κρυπτογράφησης δεν είναι ανταγωνιστικές μεταξύ τους – χρειάζονται και χρησιμοποιούνται και οι δύο.

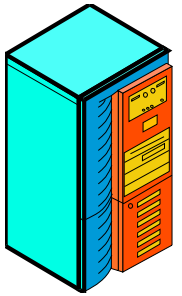
Διανομή του συμμετρικού κλειδιού κρυπτογράφηση με χρήση αλγορίθμου Δημοσίου κλειδιού



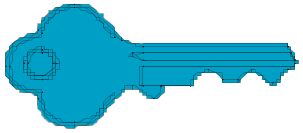
Αποστολέας Α

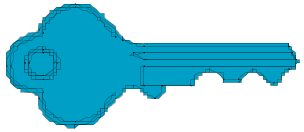
1. Δημιουργία συμμετρικού κλειδιού





Παραλήπτης Β

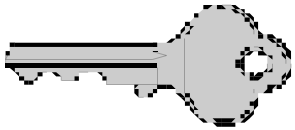




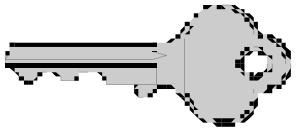
2. Κρυπτογράφηση του κλειδιού με το Δημόσιο Κλειδί του Β

3. Αποστολή του συμμετρικού κλειδιού (κρυπτογραφημένου)

4. Αποκρυπτογράφηση του συμμετρικού κλειδιού, με χρήση του Ιδιωτικού κλειδιού του Β



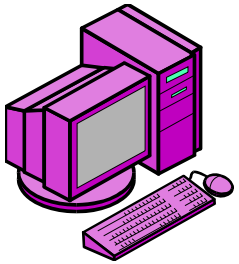
5. Χρήση του συμμετρικού κλειδιού για κρυπτογράφηση του μηνύματος



Diffie-Hellman αλγόριθμος

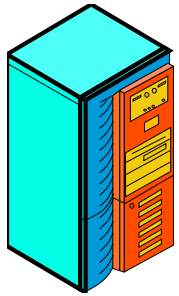
- Οι εμπνευστές της ιδέας της κρυπτογράφησης Δημοσίου Κλειδιού (Diffie, Hellman - 1976) πρότειναν μία τεχνική που να επιτρέπει την ασφαλή ανταλλαγή ενός αριθμού (μιας πληροφορίας γενικότερα) μεταξύ δύο συνδιαλεγομένων, με απώτερο στόχο ο αριθμός αυτός να χρησιμοποιηθεί μετέπειτα ως κλειδί σε κάποιον αλγόριθμο συμμετρικού κλειδιού (αλγόριθμος Diffie-Hellman).

Παράδειγμα – Diffie-Hellman μέθοδος



A

1. Συμφωνία για το Diffie-Hellman ζευγάρι p (πρώτος αριθμός) και g (γεννήτορας mod p)

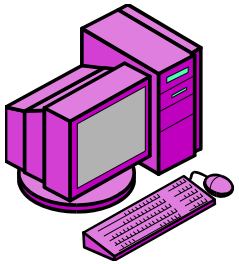


B

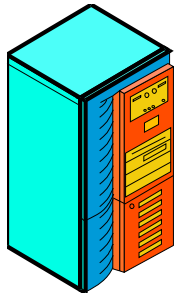
2. Δημιουργία τυχαίου αριθμού x

2. Δημιουργία τυχαίου αριθμού y

Diffie-Hellman μέθοδος (II)



A



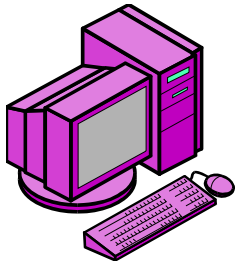
B

3.
Υπολογισμός
$x' = g^x \bmod p$

4.
Ανταλλαγή x', y'
χωρίς ασφάλεια

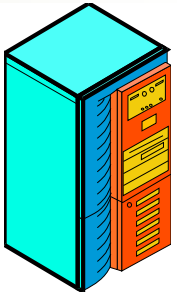
3.
Υπολογισμός
$y' = g^y \bmod p$

Diffie-Hellman μέθοδος (III)



A

5.
Υπολογισμός κλειδιού=
$y'^{x} \bmod p$
$=g^{xy} \bmod p$



B

5.
Υπολογισμός κλειδιού=
$x'^{y} \bmod p$
$=g^{xy} \bmod p$

6. Κρυπτογράφηση με το παραπάνω συμμετρικό κλειδί που υπολογίστηκε

Diffie-Hellman μέθοδος (IV)

Η ασφάλεια του Diffie-Hellman αλγορίθμου για την ανταλλαγή κλειδιού βασίζεται στη δυσκολία του προβλήματος DLP (όπως και στον El Gamal). (Γιατί??)