ΤΕΙ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΙΚΑ ΜΑΘΗΜΑΤΑ

ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ(Θ)

Ενότητα 5: ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

ΔΙΔΑΣΚΩΝ: ΚΩΝΣΤΑΝΤΙΝΟΣ ΧΕΙΛΑΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΕ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

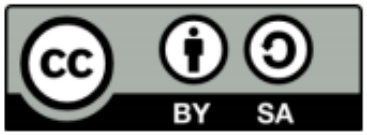
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.

- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο ΤΕΙ Κεντρικής Μακεδονίας» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ενότητα 5

ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

Χειλάς Κωνσταντίνος
Διδάκτορας Φυσικής

Περιεχόμενα ενότητας

1. Αλγόριθμοι δημόσιου κλειδιού
2. Alice και Bob
3. Επικοινωνία Αλίκης – Μπόμπου
4. Ορολογία
5. RSA
6. Επιλογή των *n*, *d* και *e*
7. Χρήση RSA
8. Άλλοι αλγόριθμοι δημόσιου κλειδιού
9. Παρεξηγήσεις σχετικά με τις ικανότητες κρυπτογράφησης δημόσιου κλειδιού

Σκοποί ενότητας

Αλγόριθμοι δημόσιου κλειδιού

Αλγόριθμοι δημόσιου κλειδιού

- Η διανομή του κλειδιού είναι ο πιο αδύναμος κρίκος στα περισσότερα κρυπτογραφικά συστήματα
- Diffie και Hellman, 1976 (Stanford Un.) πρότειναν ένα δραματικά διαφορετικό σύστημα κρυπτογράφησης.
- Στο σύστημα αυτό:

  κλειδί κρυπτογράφησης ≠ κλειδί αποκρυπτογράφησης

  και δεν υπάρχει τρόπος το ένα να προκύψει από το άλλο.
- Οι αλγόριθμοι κρυπτογράφησης, E, και αποκρυπτογράφησης, D, θα πρέπει να πληρούν τις:
  - D(E(P))=P
  - Είναι εξαιρετικά δύσκολο να συνάγεις το D από το E.
  - Ο E δεν μπορεί να σπάσει με επίθεση επιλεγμένου κειμένου

Alice και Bob

- Η Αλίκη θέλει να λαμβάνει μυστικά μηνύματα. Πρώτα πρέπει να φτιάξει δύο αλγορίθμους E_A και D_A που να πληρούν τα προηγούμενα κριτήρια.
- Μετά μπορεί να κοινοποιήσει σε οποιονδήποτε τον αλγόριθμο και το κλειδί κρυπτογράφησης (π.χ να τα βάλει στο site της).
- Αυτός είναι ο λόγος που λέγεται κρυπτογραφία δημόσιου κλειδιού
- Το ίδιο κάνει και ο Μπόμπος. Δημοσιοποιεί το δικό του E_B παραμετροποιημένο με το δημόσιο κλειδί του. Κρατάει όμως μυστικό το D_B.

Επικοινωνία Αλίκης - Μπόμπου

- Η Αλίκη και ο Μπόμπος δεν έχουν επικοινωνήσει ποτέ πριν. Η Αλίκη επιλέγει το κείμενο που θέλει να στείλει, έστω P, και το χρησιμοποιεί τον δημόσιο αλγόριθμο του Μπόμπου για να δημιουργήσει και να στείλει το $E_B(P)$. Ο Μπ. υπολογίζει το $P=D_B(E_B(P))$.
- Κανείς άλλος δεν μπορεί να υπολογίσει το P γιατί κανένας άλλος δεν έχει το D_B και επειδή τα E_B και D_B έχουν τις ιδιότητες που προαναφέραμε.
- Ο Μπ. μπορεί να απαντήσει χρησιμοποιώντας το E_A.

Ορολογία

Public key cryptography
- public key: δημόσιο κλειδί
- private key: ιδιωτικό κλειδί

Symmetric key cryptography — secret key: μυστικό κλειδί

RSA

- Ron Rivest, Adi Shamir, Len Adleman (1978, MIT)
- Έχει αντέξει σε πολλές προσπάθειες σπασίματος
- Κλειδιά μεγέθους > 1024 bits ➔ πολύ αργός σε σύγκριση με τους συμμετρικούς αλγόριθμους
- Ο RSA είναι κώδικας δέσμης (block cipher) στον οποίο το απλό και το κρυπτογραφημένο κείμενο είναι ακέραιοι από 0 έως n-1.

RSA

- Έστω M ένα κομμάτι (block) απλού κειμένου και C ένα κομμάτι (block) κρυπτογραφημένου κειμένου. Η διαδικασία κρυπτογράφησης - αποκρυπτογράφησης είναι η εξής:
  $C = M^e \bmod n$
  $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

  Το n και το e είναι γνωστά και στον αποστολέα και στον παραλήπτη, άρα αποτελούν το δημόσιο κλειδί KU$\{e, n\}$

RSA

- Το d είναι γνωστό μόνο στον παραλήπτη άρα είναι μέρος του ιδιωτικού κλειδιού KR{d, n}.
- Για να μπορεί ένας αλγόριθμος να είναι ισχυρός και υλοποιήσιμος πρέπει να ικανοποιεί τις παρακάτω απαιτήσεις:

1. Πρέπει να βρεθούν οι τιμές των e, d, n ώστε $M = M^{ed} \bmod n$ για όλα τα $M > n$.
2. Να είναι εύκολο να υπολογίσω τα C και M^e για όλες τις τιμές $M<n$.
3. Να είναι αδύνατο να υπολογίσεις το d από τα e και n.

- Οι δύο πρώτες απαιτήσεις ικανοποιούνται εύκολα, η τρίτη είναι ισχυρή μόνο για πολύ μεγάλα e και n.

Επιλογή των *n*, *d* και *e*

- Η επιλογή των *n*, *d*, *e* βασίζεται σε αρχές της θεωρίας αριθμών. Συνοπτικά η λειτουργία είναι η εξής:

1. Επέλεξε δύο μεγάλους πρώτους αριθμούς, *p* και *q* (τυπικά > 1024 bits)
2. Υπολόγισε το $n = p \times q$
3. Υπολόγισε το $\varphi(n) = (p-1)(q-1)$ (Euler totient του n)
4. Επέλεξε έναν αριθμό d, σχετικά πρώτο του $\varphi(n)$ τέτοιον ώστε $d < \varphi(n)$.
5. Βρες έναν αριθμό *e* για τον οποίο να ισχύει :
   $e \times d = 1 \bmod \varphi(n)$

Παράδειγμα 1

p=7 και q=17 → n=119, και φ(n)=96

Η παραγοντοποίηση του 96 → 2^5 x 3^1. Επομένως, ένας από τους σχετικά πρώτους αριθμούς του 96 είναι ο 5 → d=5.

d x e = 1 mod 96 → 5e = 1 mod 96 και e < 96.

Ποιοι αριθμοί διαιρούνται με το 5 και αν διαιρεθούν με το 96 θα δώσουν υπόλοιπο 1;

1 x 96 = 96 + 1 = 97

2 x 96 = 192 + 1 = 193

3 x 96 = 288 + 1 = 289

4 x 96 = 384 + 1 = 385 √

385 / 5 = 77

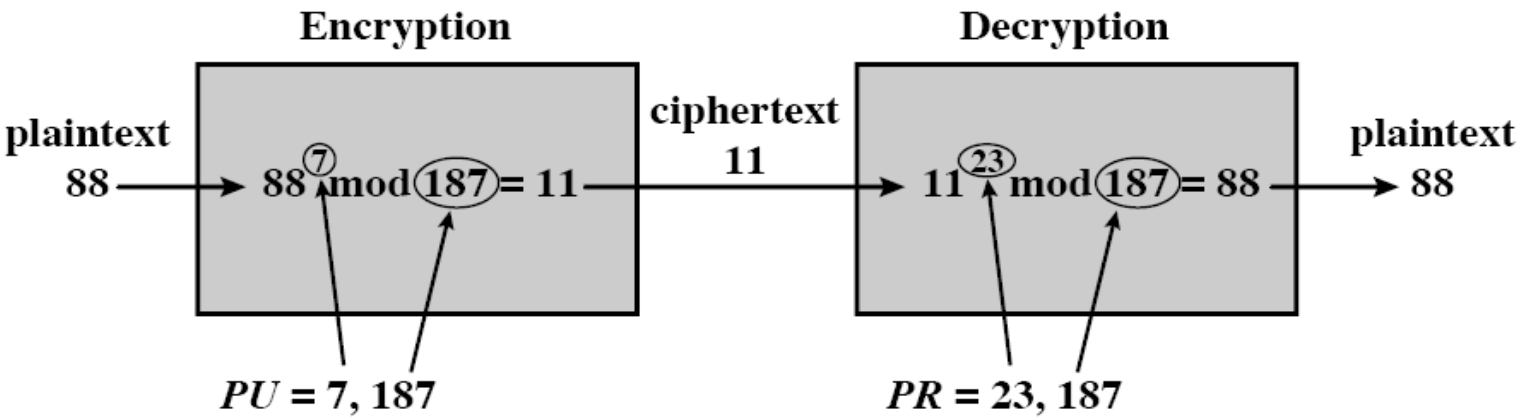
Άρα 5 x 77 = 385 = 4 x 96 + 1 = 1 mod 96

Επομένως e = 77.

public key = {5, 119}

private key = {77, 119}

Παράδειγμα 1



Παράδειγμα 2

P = 3 και q = 11 ➔ n = 33, και φ(n) = 20

Η παραγοντοποίηση του 20 ➔ 2^2 x 5^1. Επομένως, ένας από τους σχετικά πρώτους αριθμούς του 20 είναι ο 3 ➔ d = 3.

d x e = 1 mod 20 ➔ 3e = 1 mod 20 και e < 20.

Ποιοι αριθμοί διαιρούνται με το 3 και αν διαιρεθούν με το 20 θα δώσουν υπόλοιπο 1; π.χ. το 21.

Άρα 3 x 7 = 21 = 1 x 20 + 1 = 1 mod 20

Επομένως e = 7.

public key = {3, 33}

private key = {7, 33}

Παράδειγμα 2

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E
			Sender's computation		Receiver's computation	

Επειδή το n=33 και πρέπει το μέγεθος του block να είναι < 33, μπορώ να κρυπτογραφώ έναν χαρακτήρα τη φορά.
Αν όμως p και q ≈ 2^{512} οπότε n ≈ 2^{1024} μπορώ να χρησιμοποιώ blocks 1024 bits ή 128 χαρακτήρων σε αντίθεση με τα 8 bytes του DES ή τα 16 του AES

Χρήση RSA

- Ο αλγόριθμος RSA λειτουργεί σαν ECB οπότε χρειάζεται κάποια τεχνική αλύσωσης (chaining). Γενικά είναι πολύ αργός για την κρυπτογράφηση μεγάλου όγκου δεδομένων.
- Σήμερα χρησιμοποιείται κυρίως στη διαδικασία ανταλλαγής των κλειδιών μιας χρήσης στους συμμετρικούς αλγόριθμους όπως ο 3DES.

Άλλοι αλγόριθμοι δημόσιου κλειδιού

- The knapsack algorithm (Merkle και Hellman, 1978)
- Αλγόριθμοι βασισμένοι σε διακριτούς λογαρίθμους (ElGamal, 1985) (Schnorr, 1991)
- Αλγόριθμοι βασισμένοι στις ιδιότητες ελλειπτικών καμπυλών (Menezes και Vanstone, 1993)

Παρεξηγήσεις σχετικά με τις ικανότητες κρυπτογράφησης δημόσιου κλειδιού

1. Η κρυπτογραφία δημόσιου κλειδιού (ΚΔΚ) είναι πιο ισχυρή από τις συμμετρικές μεθόδους (ΚΣΚ):

   Στην πραγματικότητα η ισχύς κάθε συστήματος κρυπτογράφησης εξαρτάται:

   1. Από το μέγεθος του κλειδιού, και
   2. Από τον υπολογιστικό φόρτο για το σπάσιμο του κώδικα

2. Η ΚΔΚ έχει καταστήσει την ΚΣΚ άχρηστη.

   Αντίθετα, λόγω του υπολογιστικού φόρτου που σχετίζεται με την ΚΔΚ δεν φαίνεται να υπάρχει πιθανότητα εγκατάλειψης της ΚΣΚ στο κοντινό μέλλον

3. Υπάρχει η αίσθηση ότι η διανομή του δημόσιου κλειδιού είναι μια πολύ απλή υπόθεση, σε σύγκριση με τη διανομή συμμετρικών κλειδιών.

   Στην πραγματικότητα οι διαδικασίες που απαιτούνται δεν είναι πιο απλές ούτε πιο αποδοτικές από εκείνες της συμβατικής κρυπτογραφίας. Και εδώ απαιτείται η ύπαρξη κατάλληλου πρωτοκόλλου και πράκτορα (agent) διαμοιρασμού κλειδιών

Τέλος Ενότητας