ΤΕΙ ΗΠΕΙΡΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε
ΜΕΤΑΠΤΙΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

Ασφάλεια

ΛΙΑΓΚΟΥ ΒΑΣΙΛΙΚΗ

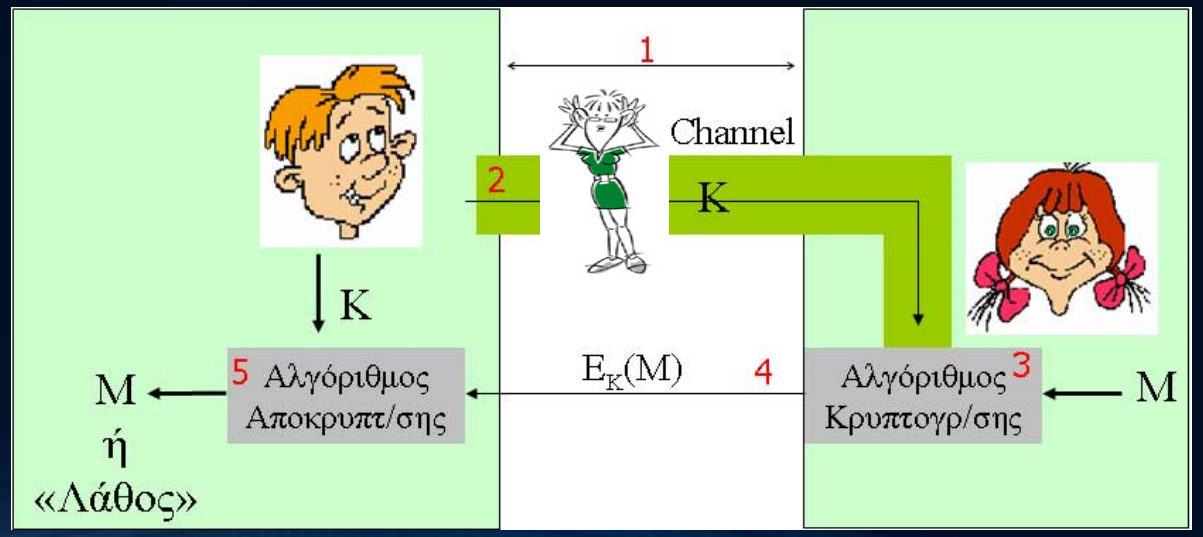
ΘΕΩΡΊΑ ΑΡΙΘΜΏΝ,
ΑΛΓΕΒΡΙΚΈΣ ΔΟΜΈΣ,
ΔΎΣΚΟΛΑ ΠΡΟΒΛΉΜΑΤΑ

Syllabus

- Μοντέλο Κρυπτογραφικής Επικοινωνίας με ΔΚ
- Ασύμμετρα Συστήματα (Ιστορία)
  - Ο αλγόριθμος του Merkle, αλγόριθμος Knapsack
- Κρυπτογραφικά Συστήματα Δημόσιου Κλειδιού
  - Ο αλγόριθμος εδραίωσης κλειδιού Diffie-Hellman
  - Ο αλγόριθμος RSA: Κρυπτογράφηση και Ψηφιακή Υπογραφή
  - Ο αλγόριθμος ElGamal: Κρυπτογράφηση και Ψηφιακή Υπογραφή
  - Ο αλγόριθμος Rabin: Κρυπτογράφηση και Ψηφιακή Υπογραφή

Από τους Συμμετρικούς Αλγορίθμους στους Αλγορίθμους Δημόσιου Κλειδιού

- Συμμετρικός αλγόριθμος ή Αλγόριθμος Μυστικού Κλειδιού
  - Το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση ($K_A = K_B = K$)
- Πρόβλημα: Πώς ανταλλάσουν το μυστικό κλειδί δυο χρήστες;
  - Το κανάλι μέσω του οποίου ανταλλάσσεται το K πρέπει να είναι ασφαλές!
    - Το Πρόβλημα της Διαχείρισης Κλειδιού (Key Management)



J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Συμμετρικά Συστήματα

Το Πρόβλημα της Διαχείρισης Κλειδιού

http://www.seiboldsecurity.com/seibold_dev_files/KeyManagement.jpg

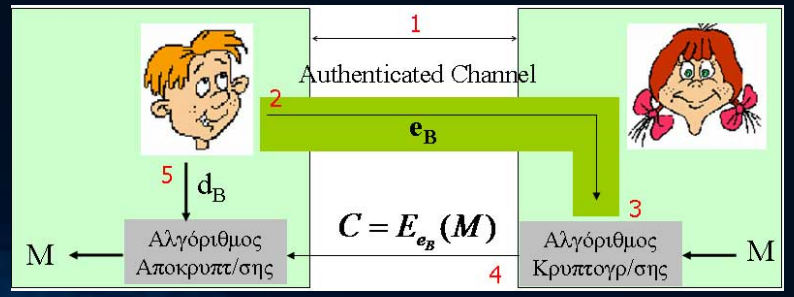
1. Ασφαλές κανάλι
   - (physically) π.χ. συνάντηση κατ' ιδίαν, μεταφορά με courier
   - (logically) - κρυπτογραφημένο
     - ... με ποιο κλειδί;

Περίπτωση: Στην επιχείρηση, ο admin διανέμει ένα κλειδί σε κάθε υπάλληλο κάθε μήνα

2. Πλήθος & αποθήκευση κλειδιών
   - π.χ. οι χρήστες δικτύου θέλουν να μπορούν όλοι να μιλούν με ασφάλεια.
     - Τι γίνεται όταν έρθει νέος υπάλληλος
   - Αν *U* οι χρήστες, κάθε χρήστης πρέπει να αποθηκεύει *U*-1 κλειδιά

3. Σε large-scale και ιδίως στο Internet, τα προβλήματα γίνονται αξεπέραστα

Solutions that are based on private-key crypto are not sufficient to deal with the problem of secure communication in open systems where the parties cannot physically meet, or when parties have transient transactions

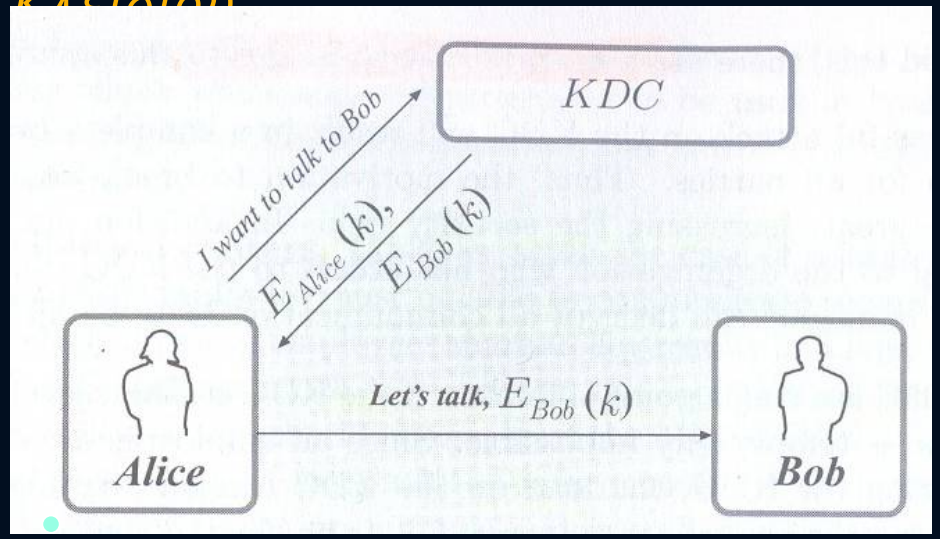


J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Το Πρόβλημα της Διαχείρισης Κλειδιού

Μία (μερική) λύση: Κέντρα Διανομής Κλειδιού

Οι χρήστες εμπιστεύονται ένα Κέντρο Διανομής Κλειδιών (KDC)



- Πλεονεκτήματα
  - Κάθε χρήστης αποθηκεύει ένα (συμμετρικό) μυστικό κλειδί
  - Απλοποιημένη διαχείριση κλειδιού
    - π.χ. πρόσληψη ή παραίτηση υπαλλήλων
- Περιπτώσεις
  - Needham-Schroeder
  - Kerberos

Ο Bob ίσως δεν είναι online: Η Alice λαμβάνει ένα ticket

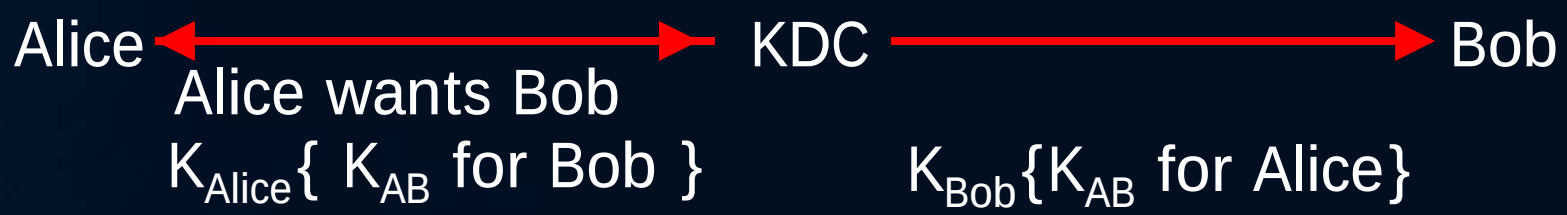
- Συζήτηση
  a) Μπορεί να υπάρχει μια οντότητα που εμπιστεύονται όλοι;
     - Ναι, σε συστήματα μικρής κλίμακας (π.χ. οργανισμός–εταιρία)
  b) Κανάλι KDC-χρήστης: Ασφαλές
     - Μπορεί η λύση να εφαρμοστεί σε Internet-Ηλ. Εμπόριο; ΟΧΙ

Kerberos

- Kerberos consists of
  - Key Distribution Center (KDC)
    - Runs on a physically secure node
  - Library of Subroutines
    - Modifies known UNIX libraries such as telnet, rlogin, …

Key Distribution Center

- KDC:
  - Database of keys for all users



  - Invents and hands out keys for each transaction between clients.

Key Distribution Center

- Message from KDC to Bob has some problems.
  - Timing problem: Alice needs to wait to make sure that Bob got the key.
  - Change the protocol so that Alice receives a *ticket* to talk to Bob.

Key Distribution Center

- Needham Schroeder:
  - Combines KDC operation with authentication.
  - Uses nonces instead of timestamps to prevent replay attacks.
    - A (sequential / random) number used only once.

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Αλγόριθμοι Δημόσιου Κλειδιού

- Συμμετρικοί αλγόριθμοι
  - Παραλληλισμός: «ένα χρηματοκιβώτιο» - ο ίδιος κωδικός χρησιμοποιείται για την εισαγωγή και εξαγωγή ενός εγγράφου

- Αλγόριθμοι Δημόσιου Κλειδιού
  - Παραλληλισμός: «ένα γραμματοκιβώτιο» - όλοι μπορούν να εισάγουν ένα έγγραφο, μόνον ο κάτοχος μπορεί να το εξάγει

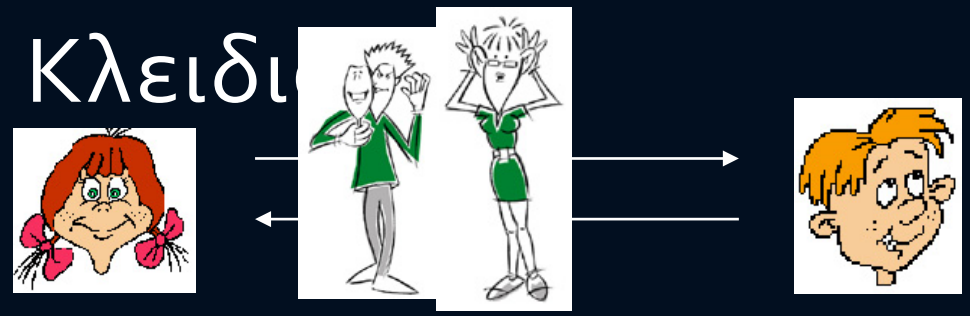
- Συναρτήσεις Μονής Κατεύθυνσης με Μυστική Πληροφορία
  - Trapdoor one-way functions
- Κρυπτογράφηση: Εύκολη
  - Οποιοσδήποτε μπορεί να κρυπτογραφήσει με το ΔΚ
- Αποκρυπτογράφηση: «Δύσκολη»
  - Μόνον αυτός που έχει το ΙΚ μπορεί να αποκρυπτογραφήσει
  - Υπολογιστική Ασφάλεια (Computational Security)

Ασυμμετρία (No1): Διαφορετικά κλειδιά χρησιμοποιούνται για κρυπτογράφηση & αποκρυπτογράφηση

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Αλγόριθμοι Δημόσιου Κλειδι

Κρυπτογράφηση



1. Η Alice και ο Bob συμφωνούν σε ένα κρυπτοσύστημα (π.χ. RSA)

<u>Κρυπτοσύστημα</u> = αλγ/θμος κρυπτογράφησης + αλγ/θμος αποκρυπτογράφησης

Ανάγκη για αυθεντικοποίηση

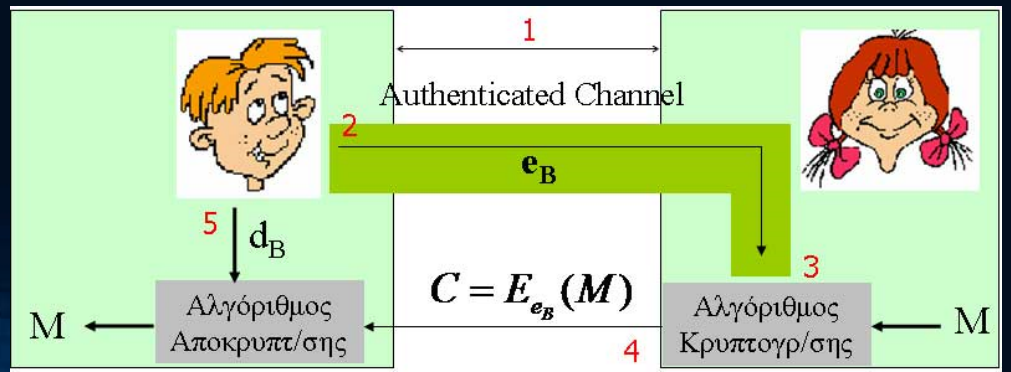
2. Ο Bob στέλνει στην Alice το ΔΚ

3. Η Alice κρυπτογραφεί το μήνυμα M με τον αλγόριθμο κρυπτογράφησης και το ΔΚ

Εναλλακτικά, η Alice θα μπορούσε να ανακτήσει το ΔΚ από μια (έγκυρη) Βάση Δεδομένων ή π.χ. από τη webpage του Bob

4. Η Alice στέλνει το κρυπτογρα-φημένο μήνυμα στον Bob

5. Ο Bob αποκρυπτογραφεί το μήνυμα με τον αλγόριθμο αποκρυπτογράφησης και το ΙΚ



Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001.

Αλγόριθμοι Δημόσιου Κλειδιού

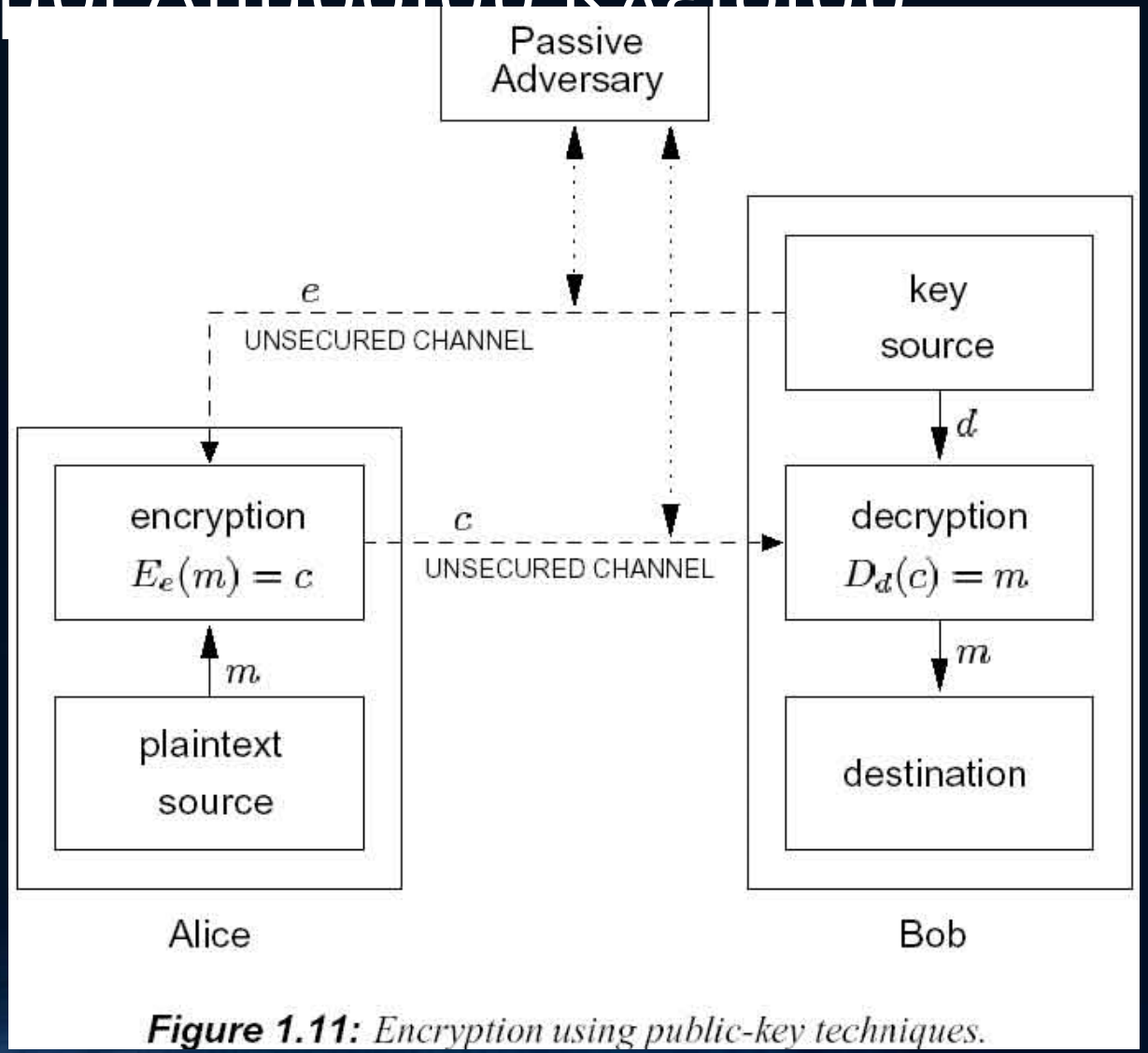
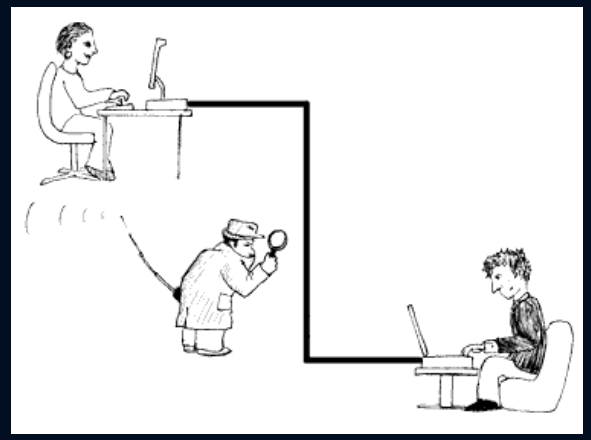
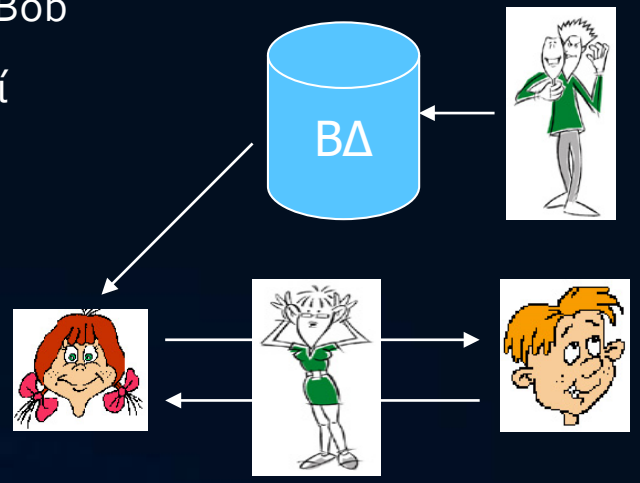


Figure 1.11: *Encryption using public-key techniques.*

Συστήματα Δημόσιου Κλειδιού Αναγκαιότητα για Αυθεντικοποίηση



- Πώς αποκτά η Alice το ΔΚ του Bob;
  1. Ο Bob της το δίνει (α) φυσικά ή (β) ηλεκτρονικά –π.χ. mail
  2. Λήψη από μια Βάση Δεδομένων ή Υπηρεσία Καταλόγου
- Σενάριο επίθεσης: (Impersonation attack)
  1. Ο Mallory αποκτά πρόσβαση στην Υπηρεσία Καταλόγου (ή στην ΒΔ) και αντικαθιστά το $ΔK_B$ του Bob με το δικό της $ΔK_M$
  2. Η Alice κρυπτογραφεί το Μ με το $ΔK_M$ και το στέλνει στον Bob
  3. Ο Mallory υποκλέπτει το μήνυμα και το αποκρυπτογραφεί

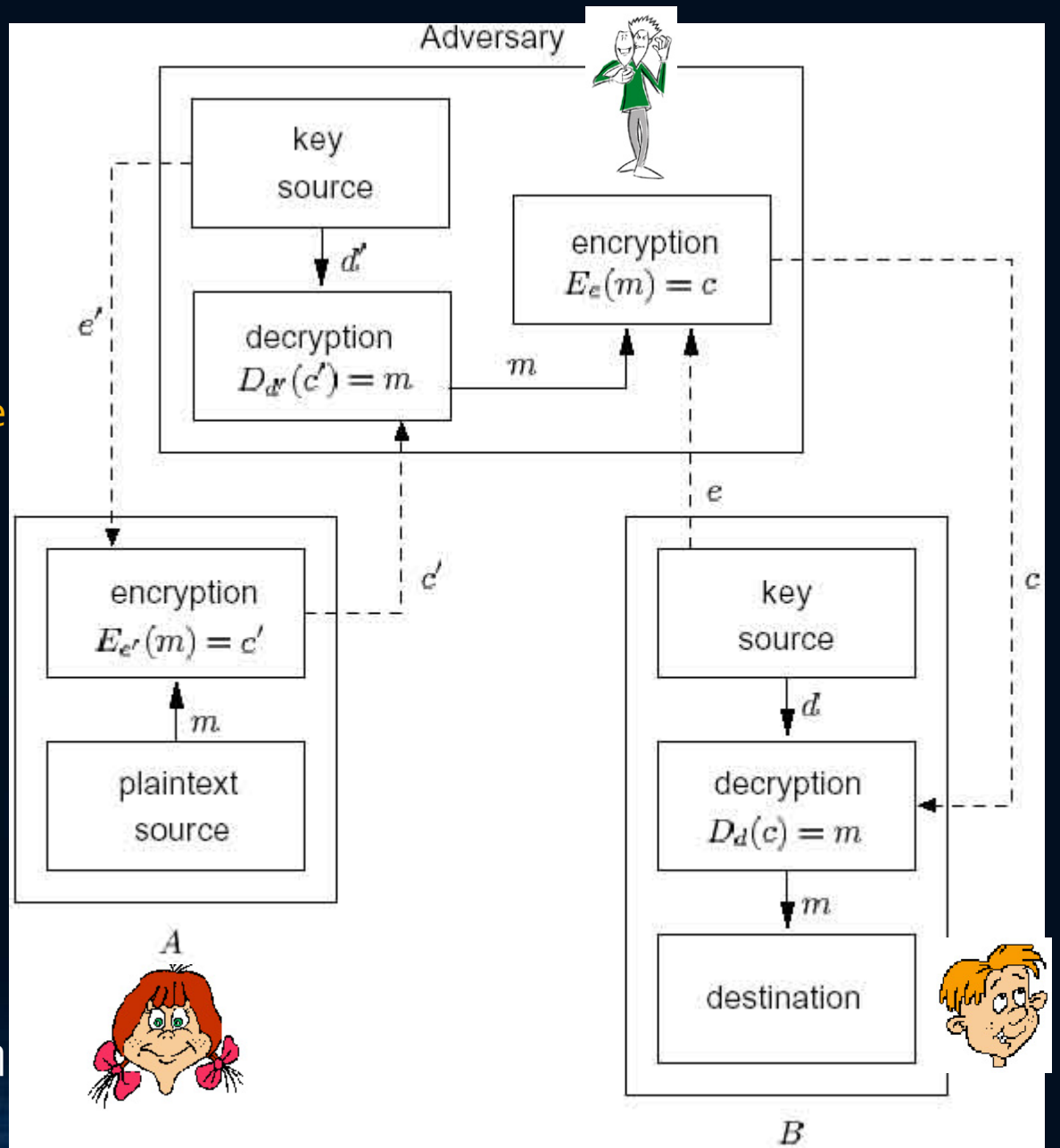


Πιθανότατα, ο Bob θα καταλάβει ότι γίνεται η επίθεση, εφόσον δεν θα μπορεί να αποκρυπτογραφήσει το μήνυμα που του έστειλε η Alice !!!

Αναγκαιότητα για Αυθεντικοποίηση

Man in the middle attack

- Ο Mallory παρεμβάλλεται στην επικοινωνία και στέλνει στην Alice το δικό του δημόσιο κλειδί αντί του Bob
- Η Alice νομίζει ότι στέλνει το μήνυμα στον Bob
- Ο Mallory μπορεί επίσης να λειτουργεί ως proxy μεταξύ του Bob και της Alice ώστε ο Bob να μην καταλάβει ότι γίνεται επίθεση

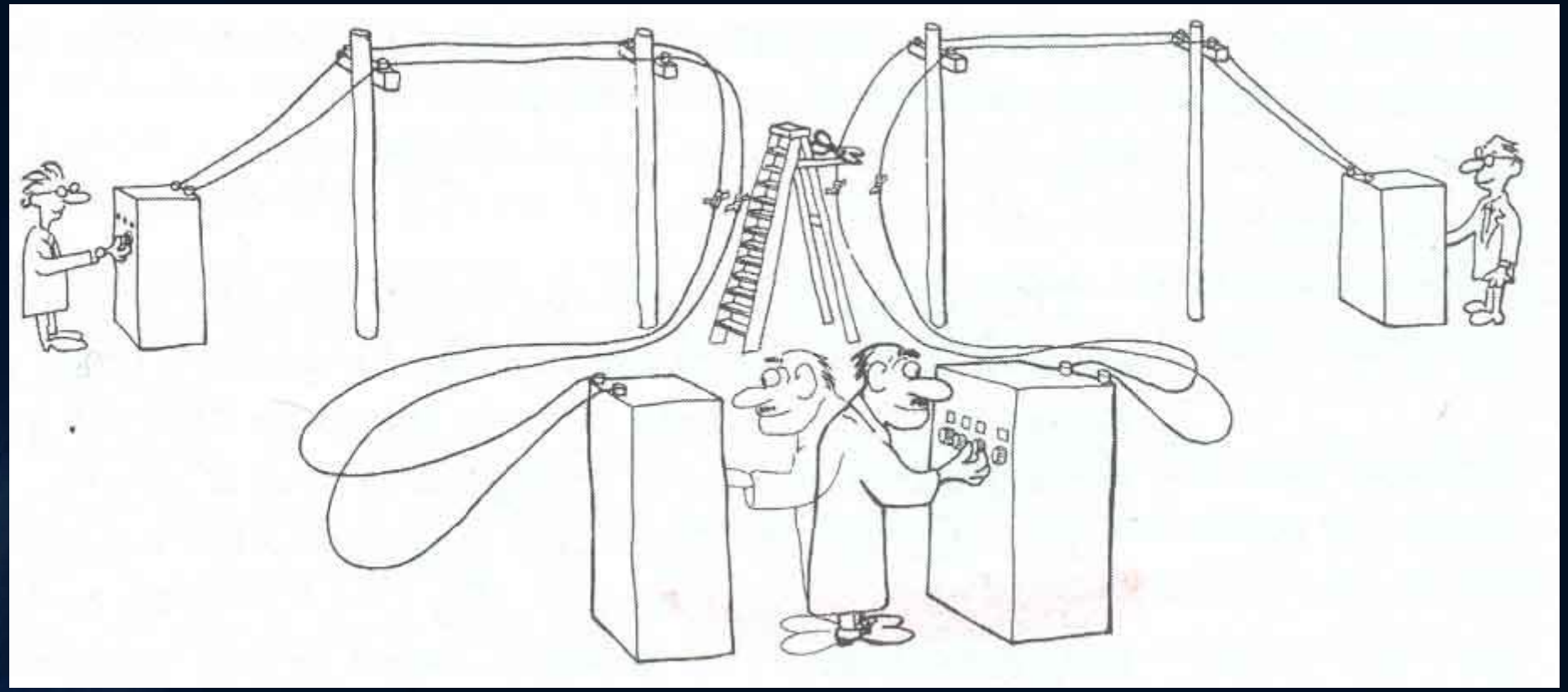


Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001.

John Hershey. Cryptography Demystified. McGraw-Hill Professional, 2003

Επιθέσεις Ενδιάμεσης Οντότητας

Man in the Middle Attacks



J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Υβριδικά Κρυπτοσυστήματα
(*Hybrid Cryptosystems*)

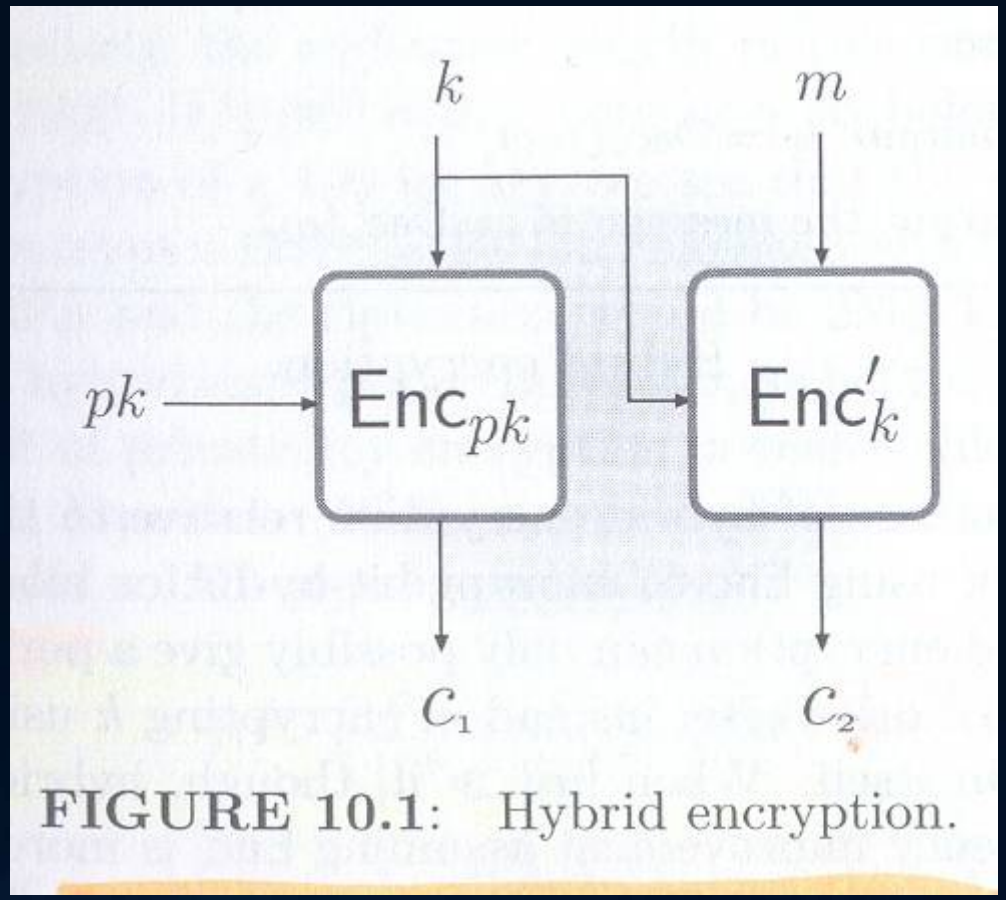


FIGURE 10.1: Hybrid encryption.

υβριδικό κρυπτοσύστημα

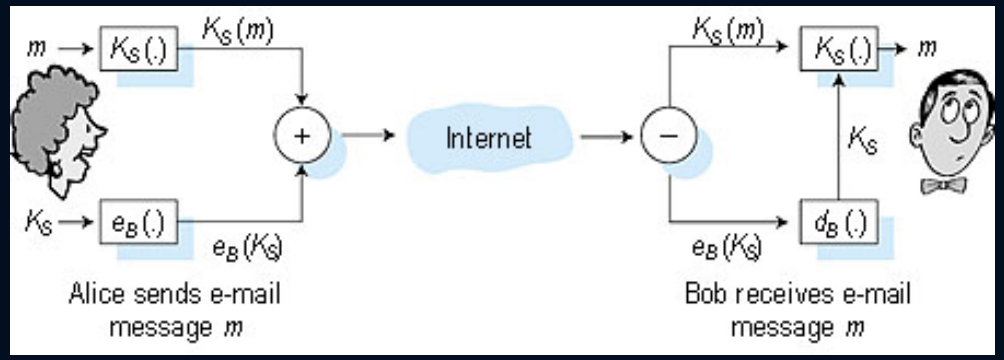
- Στην κρυπτογραφία, δημόσιου κλειδιού RSA είναι βολικό το γεγονός ότι δεν απαιτούν τον αποστολέα και παραλήπτη να μοιράζονται ένα κοινό μυστικό για να επικοινωνούν με ασφάλεια Ένα υβριδικό κρυπτογραφικό σύστημα είναι εκείνο που συνδυάζει την άνεση της κρυπτογράφησης δημόσιου με την απόδοση της συμμετρικής κρυπτογράφησης.
- Ένα υβριδικό κρυπτοσύστημα μπορεί να κατασκευαστεί χρησιμοποιώντας οποιαδήποτε δύο ξεχωριστά κρυπτοσυστήματα:
- • Κρυπτοσύστημα δημόσιου κλειδιού
- • ένα συμμετρικό κρυπτογραφικό κλειδί.

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Υβριδικά Κρυπτοσυστήματα
(Hybrid Cryptosystems)

Προβλήματα Συστημάτων ΔΚ

- Αποτελεσματικότητα – Επιδόσεις
  - Οι συμμετρικοί αλγόριθμοι είναι 1000 φορές πιο «γρήγοροι» από τους Αλγόριθμους ΔΚ
- Επιθέσεις chosen plaintext σε ντετερμινιστικά σχήματα ΔΚ



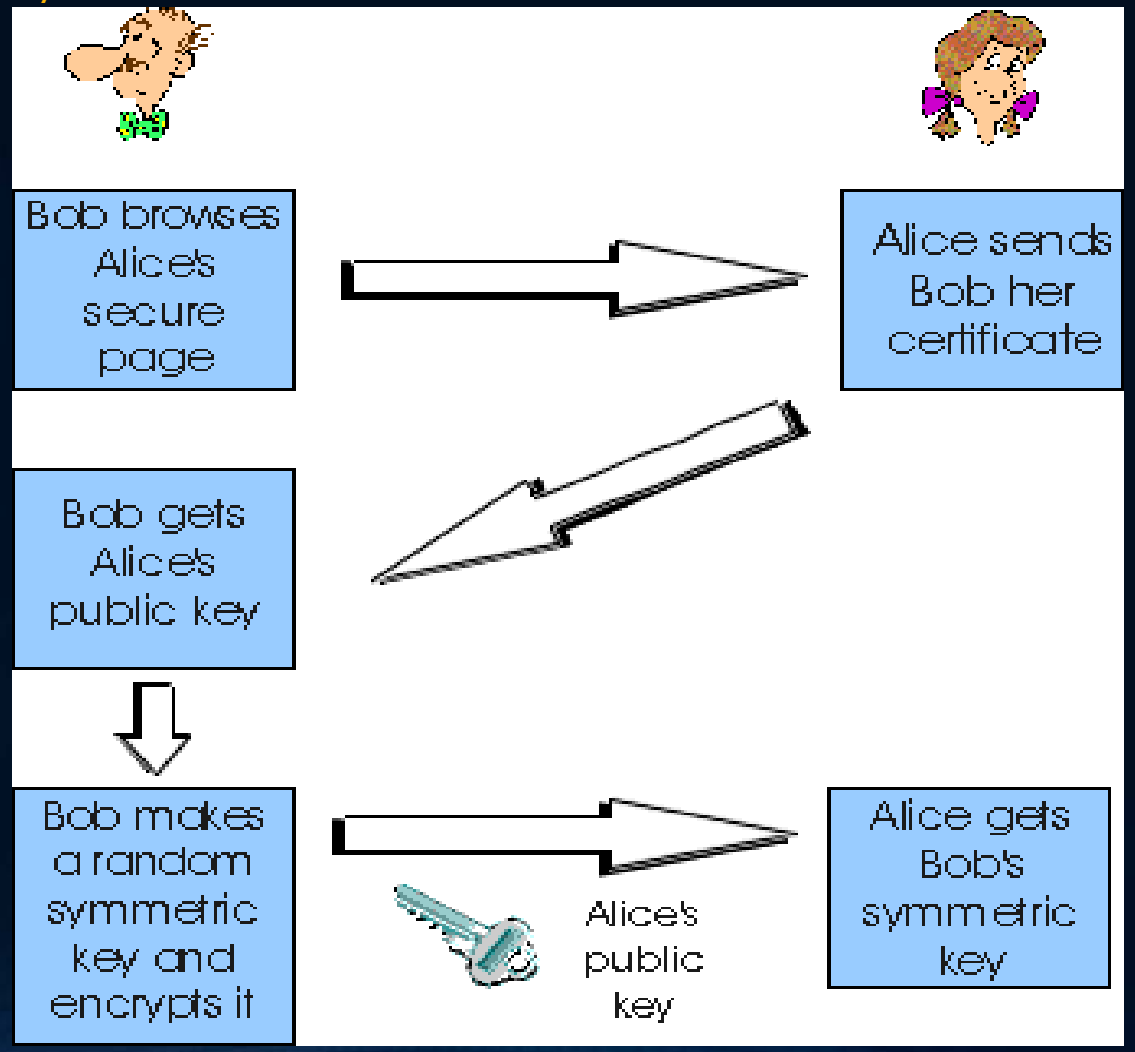
Παράδειγμα: Αν σε μια συναλλαγή το ποσό Μ κρυπτογραφείται με έναν αλγόριθμο ΔΚ, τότε το εύρος τιμών για το μήνυμα Μ είναι μικρό (π.χ. [1,…1.000.000]. Η Eve μπορεί να σπάσει το κρυπτογράφημα (brute force), κρυπτογραφώντας 500.000 τιμές (on the average)

- Τα συστήματα Δημόσιου Κλειδιού δεν ανταγωνίζονται απαραίτητα τα συστήματα Μυστικού Κλειδιού
  - Αντί για μηνύματα, τα συστήματα ΔΚ μπορούν να χρησιμοποιηθούν για να κρυπτογραφούν συμμετρικά κλειδιά

Υβριδικά (hybrid) συστήματα

Υβριδικά Κρυπτοσυστήματα

Περίπτωση: SSL/TLS



Kurose, 2003

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Μήκος «κλειδιού» στα Συστήματα ΔΚ

- Στα συστήματα ΔΚ η υπολογιστική ασφάλεια λογίζεται διαφορετικά …
- Πόσο «δύσκολο» είναι να αντιστρέψεις μια μονόδρομη συνάρτηση (one-way);
  - Π.χ. Πόσο «δύσκολο» είναι να παραγοντοποιήσεις το modulus n στους πρώτους παράγοντες p και q;
  - Π.χ. Πόσο δύσκολο είναι να βρεις το διακριτό λογάριθμο (mod p) του g^x ;
- Το μέγεθος δυσκολίας εξαρτάται από το μήκος του modulus
  - π.χ.: $\log_2(n) = 1024$ bit
- Αντιστοίχηση Συμμετρικών Συστημάτων και Συστημάτων ΔΚ ως προς το επίπεδο ασφάλειας που προσφέρουν
  - Βάσει του μήκους κλειδιού

Symmetric Key	RSA Key
56	430
80	760
96	1020
128	1620

Πηγή: RSAsecurity.com

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Μήκος «κλειδιού» στα Συστήματα ΔΚ

Recommended Public-key Key Lengths (in bits)			
Year	**vs. Individual**	**vs. Corporation**	**vs. Government**
1995	768	1280	1536
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Μήκος «κλειδιού» στα Συστήματα ΔΚ

Παραδείγματα:

1. Σε ένα υβριδικό σύστημα, έστω χρησιμοποιούμε RSA (modulus 512-bit) για τη μεταφορά ενός κλειδιού AES μήκους 256-bit

2. Σε ένα υβριδικό σύστημα, έστω χρησιμοποιούμε RSA (modulus 2048-bit) για τη μεταφορά ενός κλειδιού DES μήκους 56-bit

   - Ποια η ασφάλεια του συστήματος;

Το σύστημα είναι τόσο ασφαλές όσο το πιο «αδύνατο» κομμάτι του …

Symmetric and Public-key Key Lengths with Similar Resistances to Brute-Force Attacks

Symmetric Key Length	Public-key Key Length
56 bits	384 bits
64 bits	512 bits
80 bits	768 bits
112 bits	1792 bits
128 bits	2304 bits

Σημείωση: Σε σχέση με τα συμμετρικά συστήματα, στα συστήματα ΔΚ συνήθως επιθυμούμε η «ασφάλεια» να διαρκεί περισσότερο (π.χ. διάρκεια ζωής για ψηφιακές υπογραφές)

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Μήκος «κλειδιού»
(Γενικά)

Πόσο «μεγάλο» πρέπει να είναι το μήκος του κλειδιού;
Απάντηση (με ερώτηση):
1) Ποιος είναι ο εχθρός σου;
2) Πόση αξία έχουν τα αγαθά σου;

Security Requirements for Different Information

Type of Traffic	Lifetime	Minimum Key Length
Tactical military information	minutes/hours	56–64 bits
Product announcements, mergers, interest rates	days/weeks	64 bits
Long-term business plans	years	64 bits
Trade secrets (e.g., recipe for Coca-Cola)	decades	112 bits
H-bomb secrets	>40 years	128 bits
Identities of spies	>50 years	128 bits
Personal affairs	>50 years	128 bits
Diplomatic embarrassments	>65 years	at least 128 bits
U.S. census data	100 years	at least 128 bits

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Κρυπτογραφία Δημόσιου Κλειδιού

Public Key Cryptography

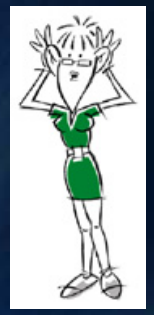
- Whitfield Diffie – Martin Hellmann

"New Directions in Cryptography," *IEEE Transactions on Information Theory*, v. IT-22, n. 6, Nov 1976, pp. 644-654.

- Ralph Merkle

"Secure Communication Over Insecure Channels," *Communications of the ACM*, v. 21, n. 4, 1978, pp. 294-299.

- «Αιώνιο» Πρόβλημα
  - Πώς θα ανταλλάξουμε με ασφάλεια ένα μυστικό κλειδί μέσω ενός μη ασφαλούς καναλιού επικοινωνίας;



Μαζί με την ψηφιακή υπογραφή, τα 2 μεγάλα πλεονεκτήματα της κρυπτογραφίας ΔΚ

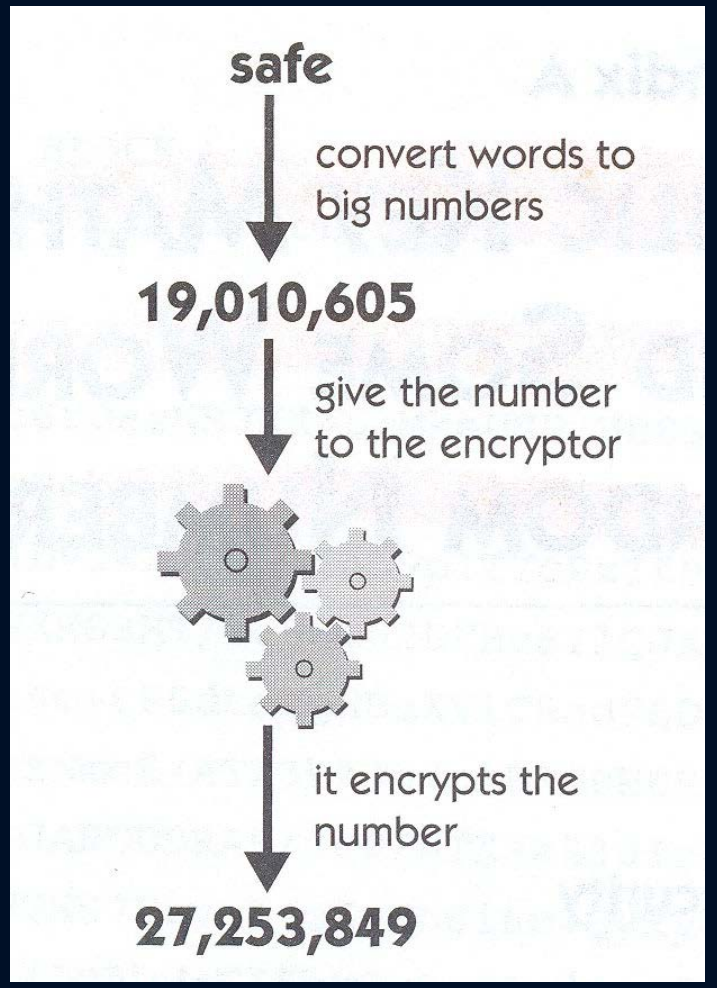
Ralph Merkle, Martin Hellman, Whitfield Diffie

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2001

Κρυπτογραφία Δημόσιου Κλειδιού

Public Key Cryptography

- Οι αλγόριθμοι δημόσιου κλειδιού μεταχειρίζονται τα δεδομένα ως αριθμούς…
- Η κρυπτογράφηση ΔΚ βασίζεται στην ύπαρξη «δύσκολων» προβλημάτων, τα οποία μπορούν να αντιστραφούν μόνον με τη χρήση μυστικής πληροφορίας
  - Μονόδρομες Συναρτήσεις Κρυφής Εισόδου (Trapdoor one-way functions)



Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Κρυπτογραφία Δημόσιου Κλειδιού

Δύσκολα Προβλήματα – & Μονόδρομες Συναρτήσεις

- $X \rightarrow f(\chi)$: «εύκολος» ο υπολογισμός
- $f(x) \rightarrow x$: «Δύσκολος» ο υπολογισμός
  - = Υπολογιστικά αδύνατος (Computationally infeasible)

It would take millions of years to compute x from f(x), even if all the computers in the world were assigned to the problem (Schneier 96)

- Ποια θα μπορούσε να είναι η χρήση των συναρτήσεων one way?
  - Κρυπτογράφηση: κανείς δεν θα μπορούσε να αποκρυπτογραφήσει το μήνυμα !
- Συναρτήσεις κρυφής εισόδου (trapdoor one-way functions)
  - One-way: Εύκολος ο υπολογισμός
  - Αντιστροφή: Δύσκολη, εκτός εάν κάποιος γνωρίζει τη μυστική πληροφορία
  - Η κρυπτογραφία δημόσιου κλειδιού βασίζεται στην ύπαρξη τους
    - π.χ RSA, Rabin, Diffie – Hellman, ElGamal,…

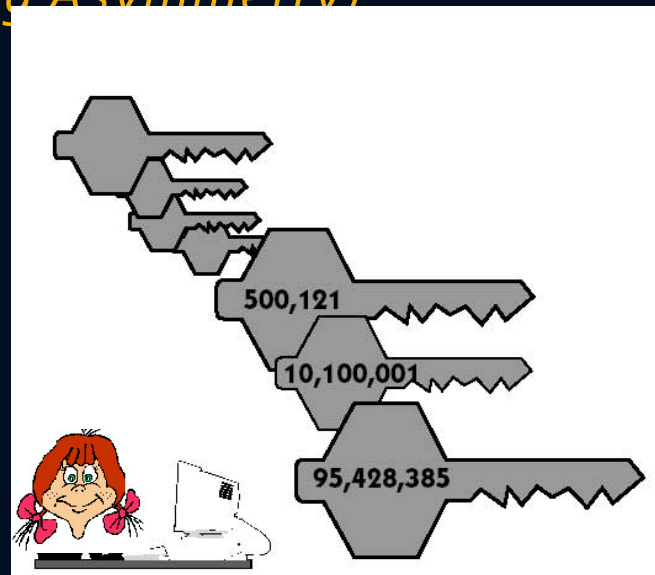
H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2000

Κρυπτογραφία Δημόσιου Κλειδιού

Η ιδέα του Merkle (Explaining Asymmetry)

1η Απόπειρα (Αποτυχημένη)

1. Η Alice φτιάχνει μια ΒΔ με 1.000.000 κλειδιά και αντίστοιχους (μοναδικούς) σειριακούς αριθμούς
2. Η Alice στέλνει στον Bob την ΒΔ
3. Ο Bob επιλέγει έναν σειριακό αριθμό (π.χ. 500.121)



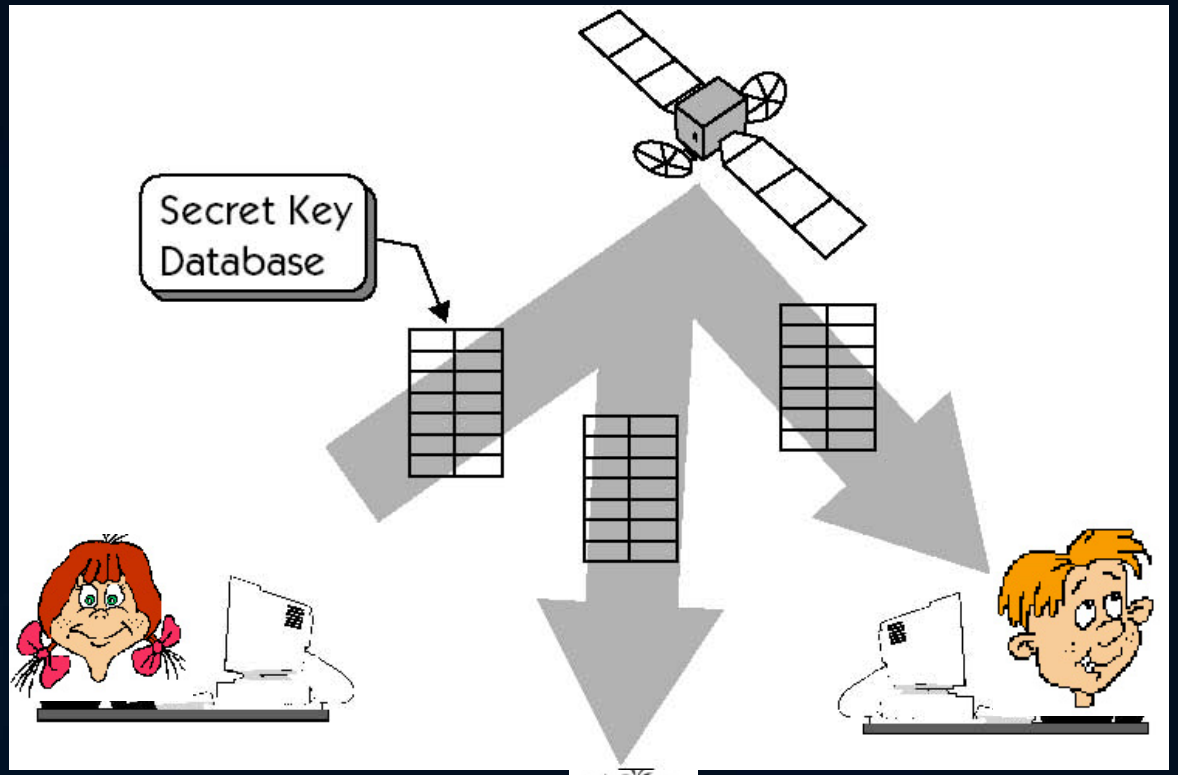
Secret Key	Serial #
aiet187f45	1,287,341
9dsyh3701	77,783,902
	…
1yt8a42x35	500,121
	…
43879d323	10,100,001
	…
25s42fds70	95,428,385

4. Ο Bob επικοινωνεί με την Alice και της λέει να χρησιμοποιήσει το κλειδί που αντιστοιχεί στον αριθμό 500.121

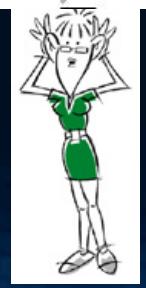
H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2000

Κρυπτογραφία Δημόσιου Κλειδιού

Η ιδέα του Merkle (Explaining Asymmetry)



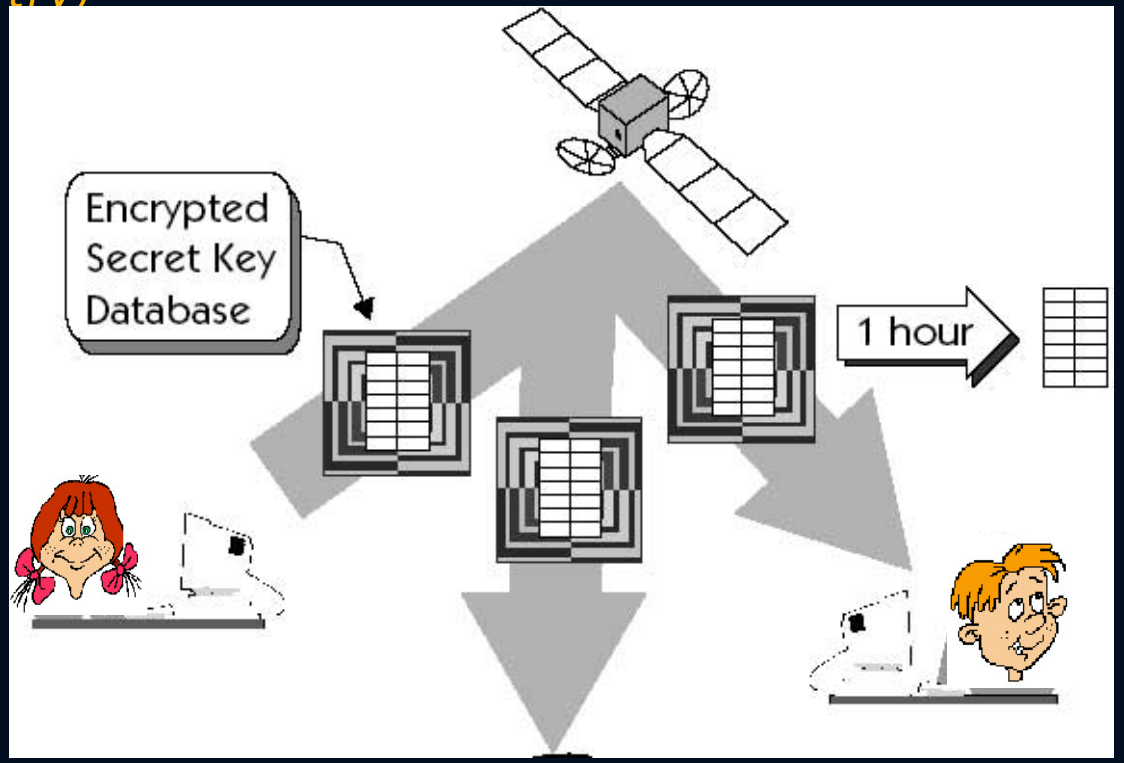
Η Eve μπορεί να υποκλέψει την επικοινωνία και να βρει το σωστό κλειδί



Κρυπτογραφία Δημόσιου Κλειδιού

H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2000

Η ιδέα του Merkle (Explaining Asymmetry)



2η Απόπειρα (Αποτυχημένη)

1. Η Alice κρυπτογραφεί την ΒΔ χρησιμοποιώντας ένα κλειδί μικρού μήκους (π.χ 20 bit)
2. Η Alice στέλνει την κρυπτογραφημένη ΒΔ στον Bob χωρίς να πει το κλειδί
3. Ο Bob πραγματοποιεί μια επίθεση brute force, βρίσκει το σωστό κλειδί και αποκρυπτογραφεί τη ΒΔ
4. Ο Bob επιλέγει έναν σειρ. αριθμό (π.χ. 500.121)

5. Ο Bob λέει στην Alice να χρησιμοποιήσει το αντίστοιχο κλειδί

Συμμετρία: Η Eve θα κάνει ό,τι ο Bob, & θα μάθει το μυστικό κλειδί

H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2000

Κρυπτογραφία Δημόσιου Κλειδιού

Η ιδέα του Merkle (Explaining Asymmetry)

1. Η Alice κρυπτογραφεί κάθε ζεύγος (συμμετρικό κλειδί | σειριακός αριθμός) της ΒΔ με διαφορετικά κλειδιά μικρού μήκους (π.χ 20 bit)

Alice Makes and Keeps			Alice Sends to Bob
Pair Number	Plaintext of Secret Key / Serial Number (reproduced from Figure 9-1)	1,000,000 Different Secret Keys—One for Each Pair Number	Encrypted Text of Secret Key/Serial Number
1	aiet187f45 / # *1,287,341*	1	Ciphertext 1
2	9dsyh3701 / # *77,183,902*	2	Ciphertext 2
3	1yt8a42x35 / # ***500,121***	3	Ciphertext 3
. . .	. . .	. . .	. . .
900,000	43879d323 / # *10,100,001*	900,000	Ciphertext 900,000
. . .	. . .	. . .	. . .
1,000,000	25s42fds70 / # *95,428,385*	1,000,000	Ciphertext 1,000,000

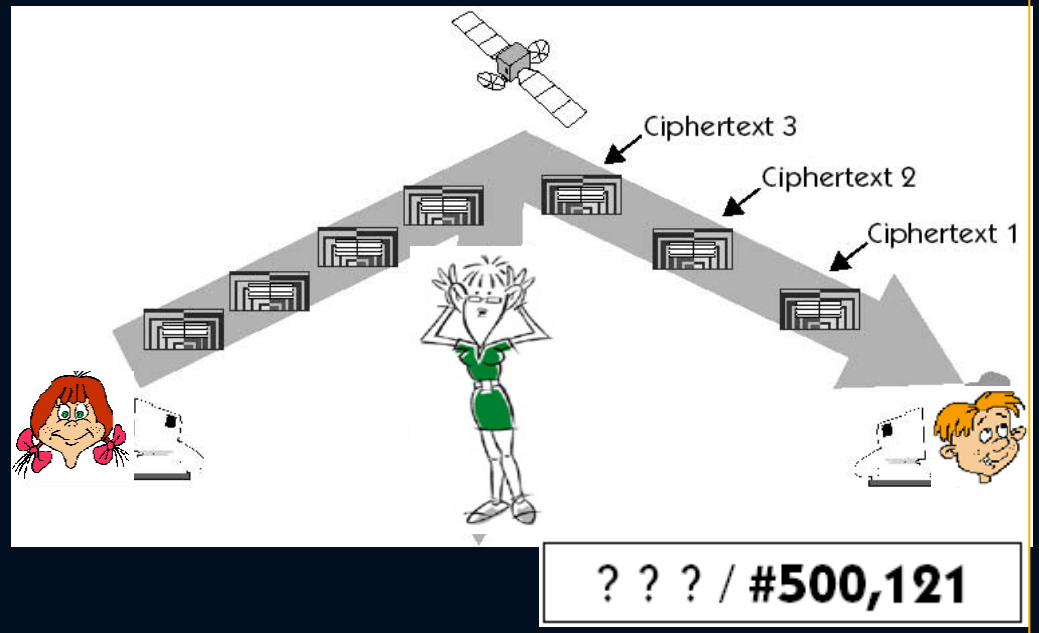
Τυχαία σειρά

H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2000

Κρυπτογραφία Δημόσιου Κλειδιού

Η ιδέα του Merkle (Explaining Asymmetry)

2. Η Alice στέλνει στον Bob 1.000.000 (~2^{20}) κρυπτογραφημένα μηνύματα
3. Ο Bob επιλέγει στην τύχη ένα μήνυμα και εξαπολύει επίθεση brute force
   - π.χ. 1 ώρας διάρκεια
4. Ο Bob ανακτά π.χ. το ζεύγος (1yt8a42x35 | 500,121)
5. Ο Bob επικοινωνεί με την Alice: της λέει να χρησιμοποιήσει το κλειδί που αντιστοιχεί στο 500.121



Ασυμμετρία (No2)

- Η Eve δεν ξέρει πιο από τα κρυπτογραφημένα μηνύματα περιέχει το κλειδί που επέλεξε ο Bob !!
- Η Eve θα πρέπει να «σπάσει» κατά μέσο όρο 2^{19} ~ 500.000 μηνύματα !!!

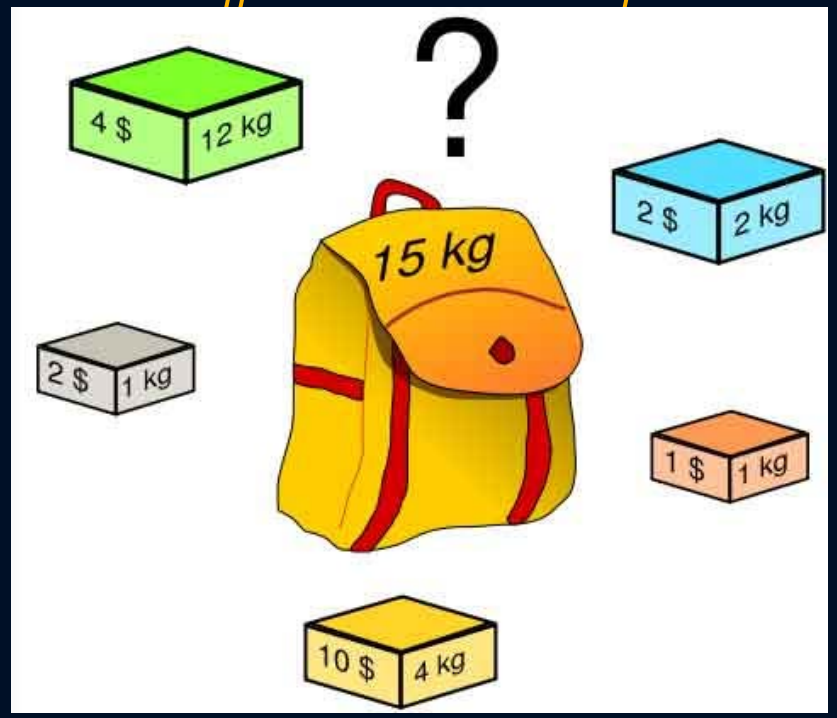
π.χ. 500.000 ώρες εργασίας

R. Merkle, M. Hellman, Hiding Information and Signatures in Trapdoor Knapsacks, IEEE Tr. Information Theory, 24(5), 1978, pp 525–530

H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2001

Κρυπτογραφία Δημόσιου Κλειδιού

Κρυπτοσυστήματα τύπου Knapsack



http://en.wikipedia.org/wiki/Knapsack_problem

Subset Sum problem

- Δοθέντος συνόλου θετικών ακεραίων $\{a_1, a_2, \ldots, a_n\}$ και ενός θετικού ακεραίου s, έλεγχος για το αν υπάρχει ή όχι υποσύνολο των a_i τέτοιων ώστε το άθροισμά τους να ισούται με s.

- SUBSET-SUM: Πρόβλημα NP-Complete
  - Ωστόσο, κάποια στιγμιότυπα του προβλήματος είναι εύκολα (=λύνονται αποδοτικά)
  - Ιδέα: Κωδικοποιούμε ένα μήνυμα ώστε ο παραλήπτης (και μόνον), να λύσει ένα εύκολο στιγμιότυπο

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2001

Κρυπτογραφία Δημόσιου Κλειδιού

Ο αλγόριθμος Knapsack (Merkle-Hellman)

- Η Alice δίνει πληροφορίες-προβλέψεις για μετοχές εισηγμένων εταιριών, στους πελάτες της

ALICE'S HOT PICKS

Select and Sum Stock Numbers

Name	Number
Amazon.com	1
Barnes & Noble	3
Ford Motor	5
General Motors	10
IBM	20
Microsoft	40

Figure 11-3 Alice sends her clients a list of stocks with special numbers that they can use to encipher the information.

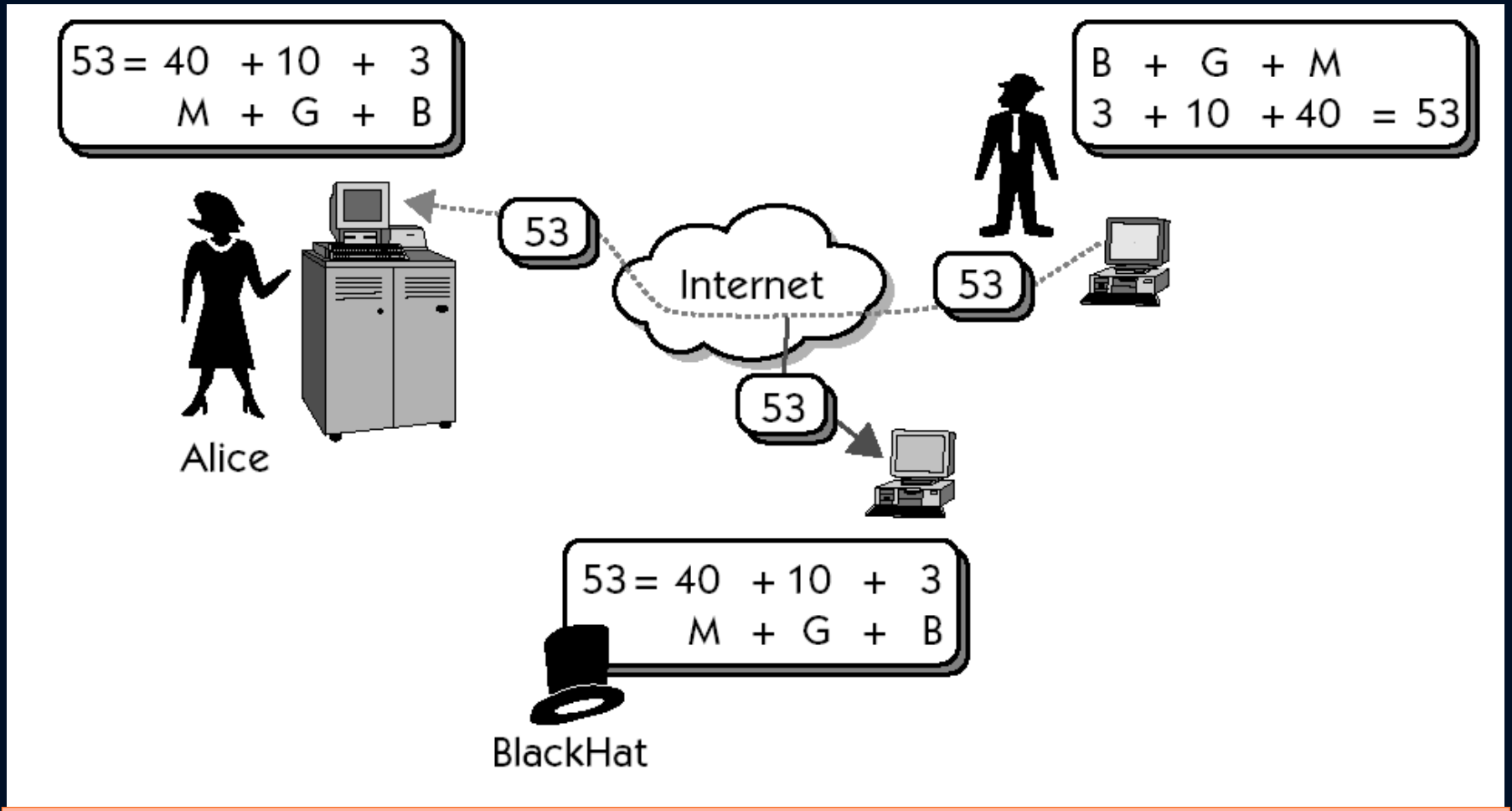
- Οι πελάτες της Alice απαιτούν μυστικότητα στις μετοχές που διαλέγουν για να πληροφορηθούν… ας δούμε το πρωτόκολλο:
  1. Κάθε εταιρία κωδικοποιείται με έναν αριθμό
  2. Η λίστα με τους αριθμούς δημοσιεύεται στο Internet
  3. Ο πελάτης υπολογίζει και στέλνει στην Alice το άθροισμα των αριθμών των μετοχών που τον ενδιαφέρουν…

  Μπορεί να το κάνει με μυστικότητα?

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2001

Κρυπτογραφία Δημόσιου Κλειδιού

Ο αλγόριθμος Knapsack (Merkle, Hellman)



Ο Blackhat υποκλέπτει την επικοινωνία και φτιάχνει τους σωστούς αριθμούς

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2001

Κρυπτογραφία Δημόσιου Κλειδιού

Ο αλγόριθμος Knapsack (Merkle, Hellman)

Private Key (super-increasing sequence)	*23	Public Key mod 101
1	23	23
3	69	69
5	115	14
10	230	28
20	460	56
40	920	11

Ένα διάνυσμα $(\alpha_1, \alpha_2, \dots, \alpha_n) \theta\alpha\ \lambda\varepsilon\gamma\varepsilon\tau\alpha\iota\ super - increasing\ sequence\ \alpha\nu\ a_j > \sum a_i$ για i:1,…,j-1 με j<=n

Γένεση Κλειδιού

- Επέλεξε μια $super - increasing\ sequence$ $(\alpha_1, \alpha_2, \dots, \alpha_n)$
- Διάλεξε έναν αριθμό q τέτοιο ώστε q> $\sum a_i$ για i:1,…,j-1 με j<=n, το q θα λέγεται modulus
- Διάλεξε ένα r που μεταξύ τους να είναι πρώτο gcd(r,q)=1, το r θα είναι ο πολλαπλασιαστής
- Υπολόγισέ ένα διάνυσμα b_i: $(b_1, b_2, \dots, b_n)$ τέτοιά ώστε:$b_i = ra_i mod(q), 0 \leq b_i < q$

Τα κλειδιά:
Δημόσιο: b_i
Ιδιωτικό: (a_i, q, r)

Η Alice «κατασκευάζει» ένα δημόσιο κλειδί από ένα ιδιωτικό, χρησιμοποιώντας αντιστρόφους modulo n

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2001

Κρυπτογραφία Δημόσιου Κλειδιού

Ο αλγόριθμος Knapsack (Merkle, Hellman)

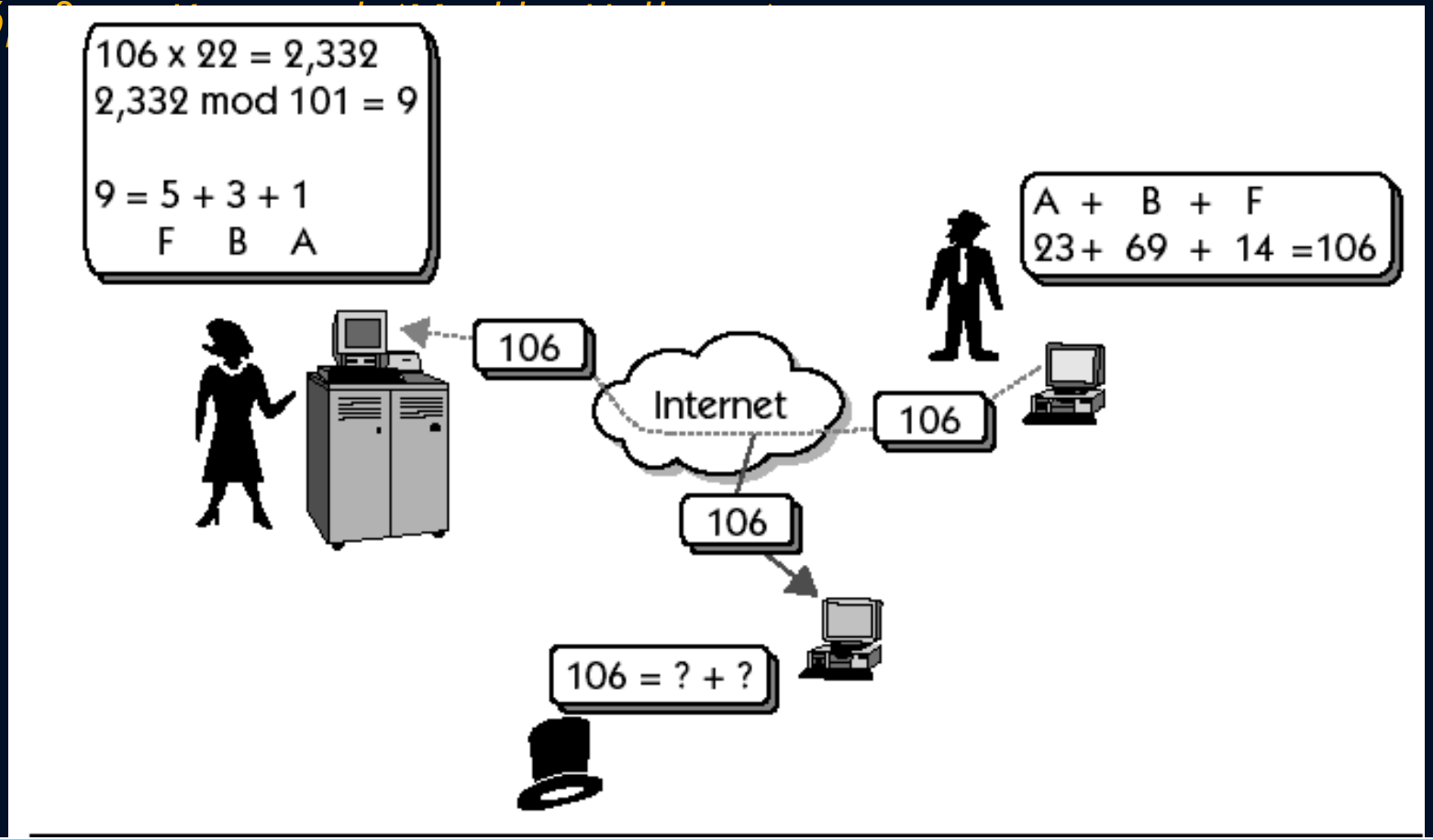
Name	Private Key (not disclosed)	Public Key (openly distributed) select and sum stock numbers
Amazon.com	1	23
Barnes & Noble	3	69
Ford Motor	5	14
General Motors	10	28
IBM	20	56
Microsoft	40	11

Το ιδιωτικό (private) και δημόσιο (public) κλειδί της Alice

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2001

Κρυπτογραφία Δημόσιου Κλειδιού

Ο αλγό



Η Alice μετατρέπει ένα «δύσκολο» πρόβλημα σε «εύκολο» (γιατί ξέρει το trapdoor)

Ο Blackhat θα πρέπει να λύσει το «δύσκολο» πρόβλημα –Ασύμμετρη Κρυπτογραφία

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2001

Κρυπτογραφία Δημόσιου Κλειδιού

Ο αλγόριθμος Knapsack (Merkle, Hellman)

Private Key	Public Key			Private Key
	(Column 1 x 23)	(Column 2 mod 101)	(Column 3 x 22)	(Column 4 mod 101)
1	23	23	506	1
3	69	69	1,518	3
5	115	14	308	5
10	230	28	616	10
20	460	56	1,232	20
40	920	11	242	40

Figure 11-21 Alice manufactures a public key from her private key, and then, to show it's reversible, she converts her public key back to her private key using her modulo inverse pair 23 x 22 mod 101.

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2000

Κρυπτογραφία Δημόσιου Κλειδιού

Το Πρωτόκολλο «Ανταλλαγής Κλειδιού» των Diffie-Hellman

- 1976: Το πρώτο (με δίπλωμα ευρεσιτεχνίας) κρυπτογραφικό σύστημα Δημόσιου Κλειδιού
- Η Alice και ο Bob φτιάχνουν από κοινού ένα μυστικό κλειδί, γνωρίζοντας ότι κάποιος μπορεί να παρακολουθεί τη συνομιλία

Παράδειγμα: Μπορούν η Alice και ο Bob, χωρίς να έχουν συναντηθεί ή επικοινωνήσει νωρίτερα, να βρεθούν σε ένα δωμάτιο, παρούσης της Eve, και να μιλήσουν με μυστικότητα ? !!!

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2000

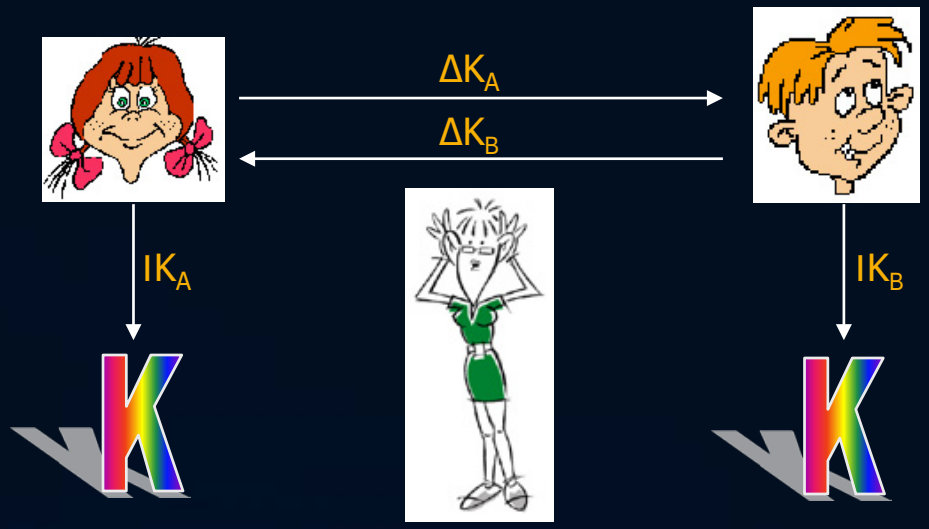
Κρυπτογραφία Δημόσιου Κλειδιού

Το Πρωτόκολλο «Ανταλλαγής Κλειδιού» των Diffie-Hellman

Το πρωτόκολλο

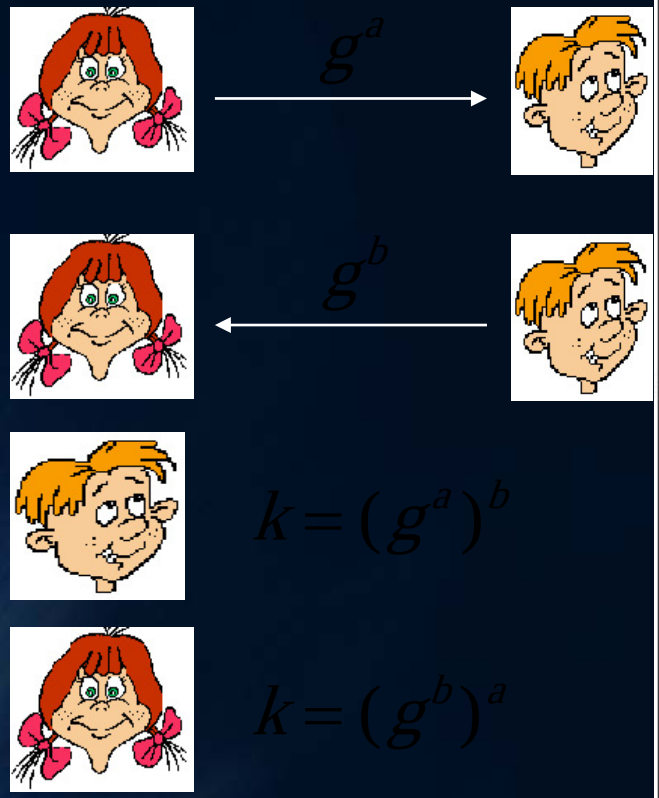
- Η Alice και ο Bob διαθέτουν (ο καθένας ξεχωριστά):
  - ένα Ιδιωτικό (ΙΚ) Κλειδί
  - ένα Δημόσιο (ΔΚ) Κλειδί

1. Η Alice και ο Bob ανταλλάσσουν τα δημόσια κλειδιά τους ΔK_A, ΔK_B
2. Η Alice συνδυάζει το ιδιωτικό της κλειδί IK_A με το ΔK_B του Bob και υπολογίζει το μυστικό κλειδί K
3. Ο Bob συνδυάζει το ιδιωτικό του κλειδί IK_B με το ΔK_A της Alice και υπολογίζει το μυστικό κλειδί K



H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2000

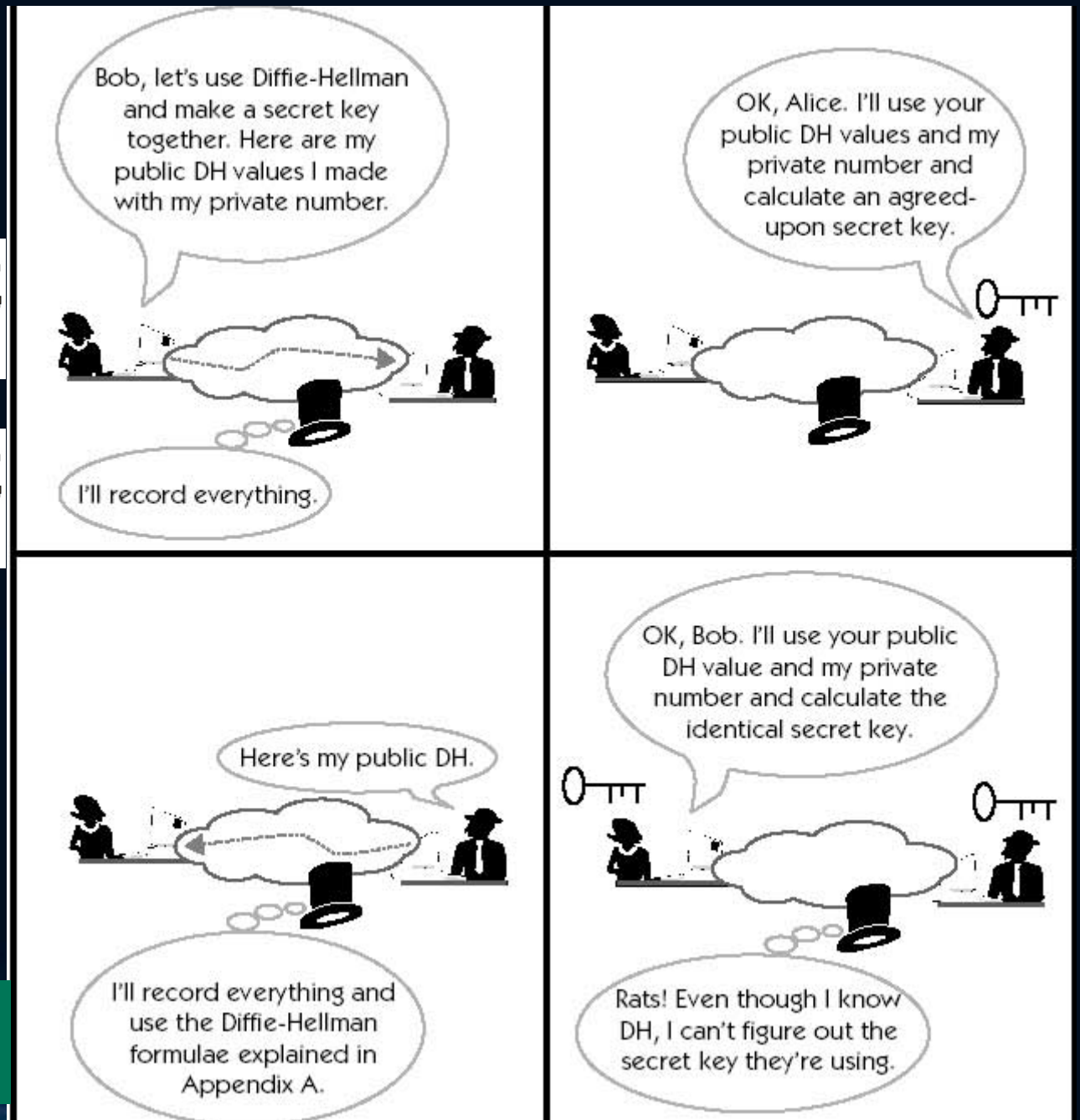
Το Πρωτόκολλο Diffie-Hellman



Όλες οι πράξεις γίνονται mod p

g: Γεννήτορας της (Z*p, x)

p: Μεγάλος Πρώτος Αριθμός



Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Κρυπτογραφία Δημόσιου Κλειδιού

Το Πρωτόκολλο «Ανταλλαγής Κλειδιού» των Diffie-Hellman

Protocol Diffie-Hellman key agreement (basic version)

SUMMARY: A and B each send the other one message over an open channel.
RESULT: shared secret K known to both parties A and B.

1. *One-time setup.* An appropriate prime p and generator α of $\mathbb{Z}_p^*$ ($2 \leq \alpha \leq p-2$) are selected and published.
2. *Protocol messages.*

$$A \rightarrow B : \alpha^x \bmod p \quad (1)$$
$$A \leftarrow B : \alpha^y \bmod p \quad (2)$$

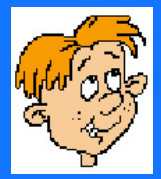
3. *Protocol actions.* Perform the following steps each time a shared key is required.
   (a) A chooses a random secret x, $1 \leq x \leq p-2$, and sends B message (1).
   (b) B chooses a random secret y, $1 \leq y \leq p-2$, and sends A message (2).
   (c) B receives α^x and computes the shared key as $K = (\alpha^x)^y \bmod p$.
   (d) A receives α^y and computes the shared key as $K = (\alpha^y)^x \bmod p$.

John Hershey. Cryptography Demystified. McGraw-Hill Professional, 2003

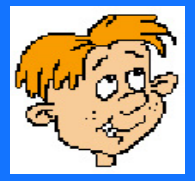
Κρυπτογραφία Δημόσιου Κλειδιού

Το Πρωτόκολλο Diffie-Hellman – Αριθμητικό παράδειγμα


g^a

g^b



$k = (g^a)^b$

$k = (g^b)^a$

Όλες οι πράξεις γίνονται mod p

g και p: Παράμετροι συστήματος

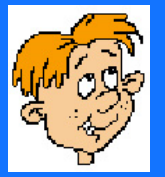
ΓΝΩΣΤΕΣ ΣΕ ΟΛΟΥΣ

Παράμετροι συστήματος

p= 101, g=3

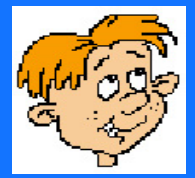
a=5

$3^5 \bmod 101 = 41$



b=6

$3^6 \bmod 101 = 22$



$k = 41^6 \bmod 101 = 6$

$k = 22^5 \bmod 101 = 6$

Το Πρωτόκολλο Diffie-Hellman

Ασφάλεια του πρωτοκόλλου DH – Η υπόθεση CDH

- Η υπόθεση CDH (Computational Diffie Hellman)

Δεδομένων μια ομάδας G, ενός γεννήτορα g, και των τιμών g^x, g^y, όπου x, y είναι τυχαίοι εκθέτες, είναι υπολογιστικά αδύνατο για την Eve να υπολογίσει την τιμή g^{xy}

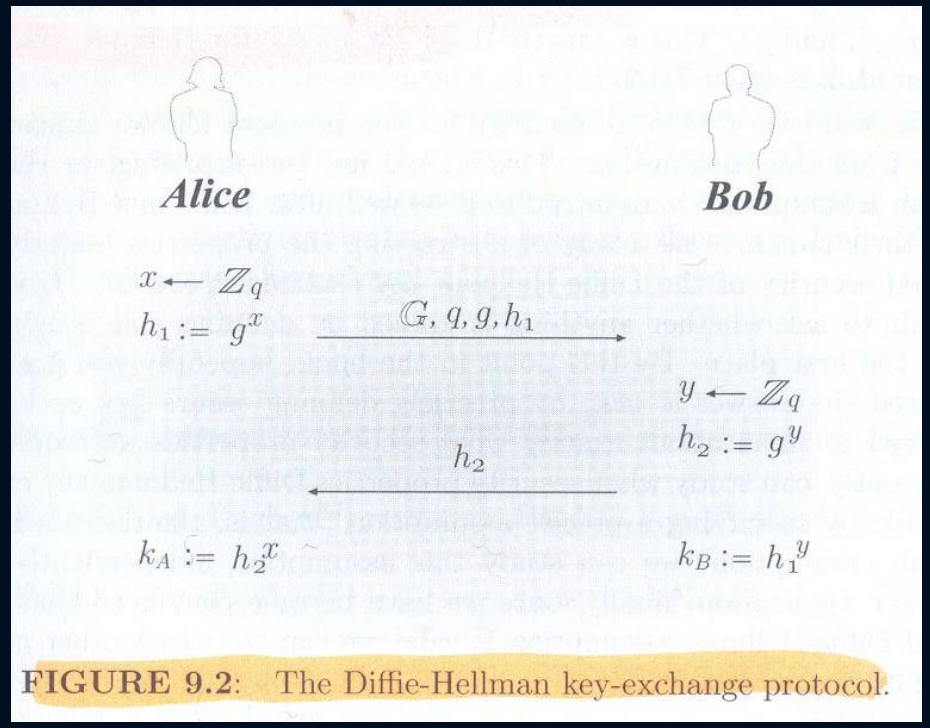


FIGURE 9.2: The Diffie-Hellman key-exchange protocol.

- Αναγωγή στο πρόβλημα Διακριτού Λογάριθμου (DL problem)
  - Εύρεση διακριτών λογαρίθμων όταν το modulus p είναι μεγάλος πρώτος
    - π.χ. Μήκος(p) = 1024 bit

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

A. Young, M. Yung. Malicious Cryptography – Exploring CryptoVirology. Wiley, 2004

Το Πρωτόκολλο Diffie-Hellman

(Σημασιολογική) Ασφάλεια του πρωτοκόλλου DH

- Το πρόβλημα Απόφασης DDH (Decisional Diffie Hellman)

Δίνονται: G, g, q (οι παράμετροι του πρωτοκόλλου), g^x, g^y (οι τιμές που ανταλλάσσονται), και g^z (μια υποψήφια λύση). Αποφάσισε: Ισχύει $g^z = g^{xy}$, ή το z είναι μια τυχαία τιμή στο G;

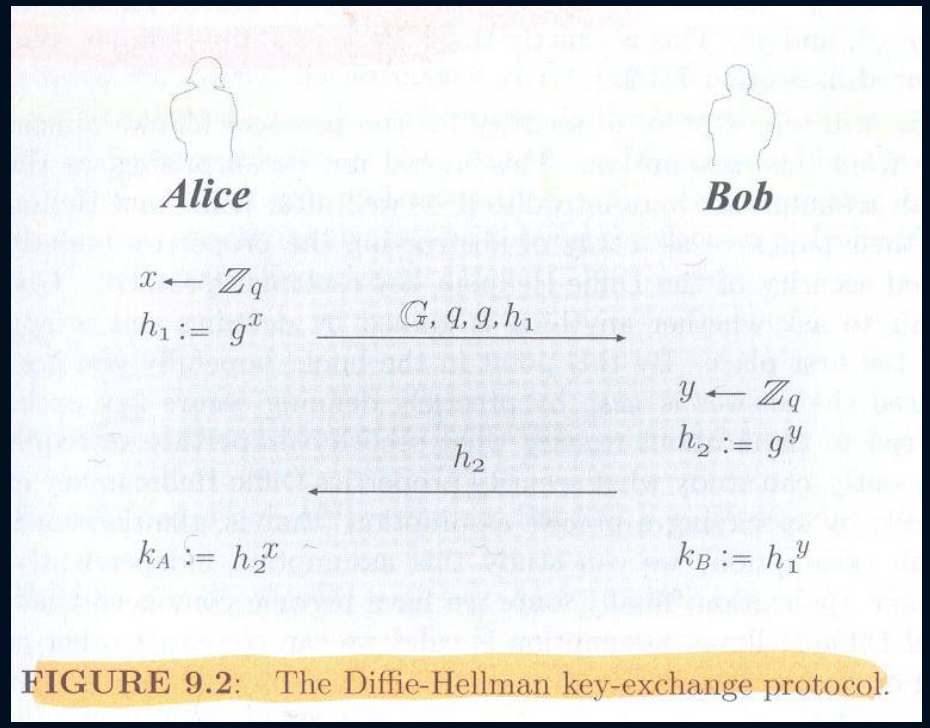


FIGURE 9.2: The Diffie-Hellman key-exchange protocol.

- Επίσης, αναγωγή στο πρόβλημα Διακριτού Λογάριθμου (DL problem)

A. Young, M. Yung. Malicious Cryptography – Exploring CryptoVirology. Wiley, 2004

Κρυπτογραφία Δημόσιου Κλειδιού

Το Πρωτόκολλο Diffie-Hellman

Συζήτηση: Ασφάλεια

1. Το πρωτόκολλο προστατεύει τους χρήστες από την Eve
   - Ωστόσο όχι και από τον Mallory…
- Δεν υπάρχει αυθεντικοποίηση
  - π.χ. Η Alice δεν είναι σίγουρη ότι μιλάει με τον Bob
    - Impersonation attacks,
    - Man In the Middle attacks,…
  - Το πρόβλημα αντιμετωπίζεται αν ο Bob και η Alice υπογράψουν ψηφιακά τα μηνύματα τους
    - Π.χ. S2S protocol

Συζήτηση: Διαχείριση κλειδιού

2. DH: Πρωτόκολλο ανταλλαγής συμμε-τρικού κλειδιού (Key Agreement)
   - Ο αριθμός των κλειδιών σε ένα δίκτυο *U* χρηστών, παραμένει ο ίδιος !

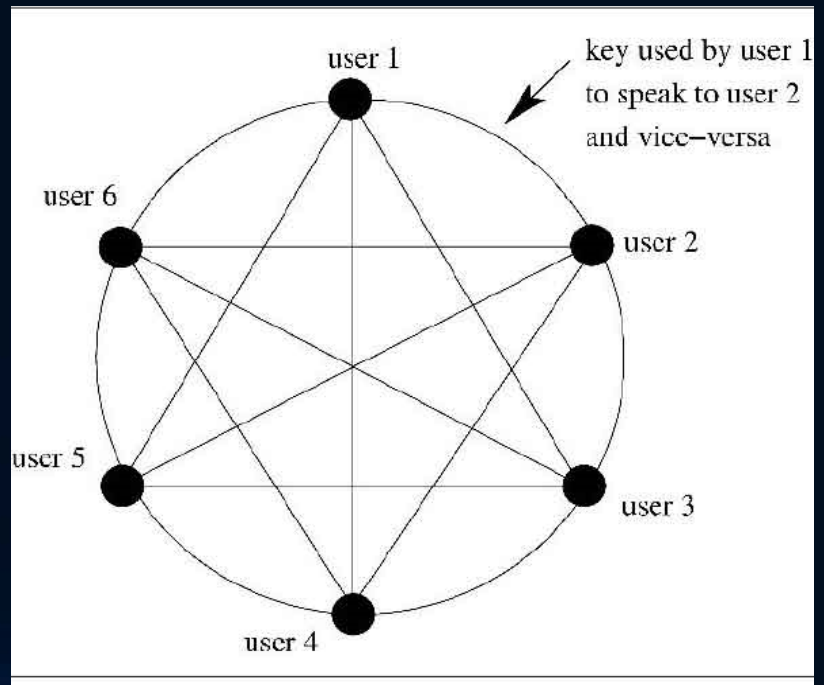


Figure C.1 Symmetric keys needed for six users

Επίθεση Ενδιάμεσης Οντότητας (MIM) στο πρωτόκολλο Diffie-Hellman

N. Ferguson, B. Schneier. Practical Cryptography. Wiley, 2003.

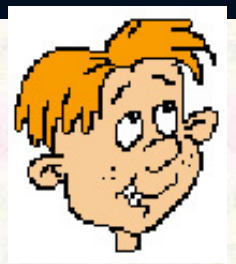


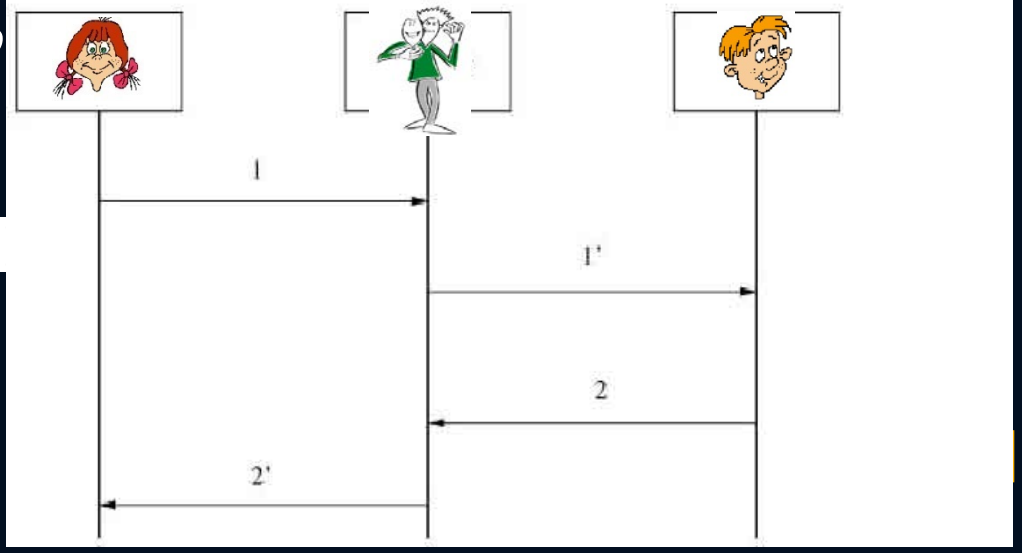
Figure 12.2: Diffie-Hellman protocol with a man in the middle.

Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

Επίθεση Ενδιάμεσης Οντότητας στο πρωτόκολλο Diffie-Hellman

Attack 8.1: Man-in-the-Middle Attack on the Diffie-Hellman Key Exchange Protocol

COMMON INPUT: Same as Prot 8.1.



1. Η Alice επιλέγει έναν τυχαίο αριθμό $a \in_U [1, p-1]$ υπολογίζει και στέλνει $g_a \leftarrow g^a \pmod p$ στον Mallory ("Bob")

2. Ο Mallory ("Alice") υπολογίζει $g_m \leftarrow g^m \pmod p$ για κάποιο $m \in [1, p-1]$ και στέλνει στον Bob g_m

3. Ο Bob επιλέγει $b \in_U [1, p-1]$, υπολογίζει και στέλνει το $g_b \leftarrow g^b \pmod p$ τον Mallory ("Alice") g_b

4. Ο Mallory ("Bob") στέλνει το g_m στην Alice

5. Η Alice υπολογίζει $k_1 \leftarrow g_m^a (\mathrm{mod} p)$
   - Το κλειδί αυτό θα το μοιράζεται εφεξής με τον Mallory, ο οποίος επίσης υπολογίζει $k_1 \leftarrow g_a^m (\mathrm{mod} p)$

6. Ο Bob υπολογίζει $k_2 \leftarrow g_m^b (\mathrm{mod} p)$
   - Το κλειδί αυτό θα το μοιράζεται εφεξής με τον Mallory, ο οποίος επίσης υπολογίζει $k_2 \leftarrow g_m^b (\mathrm{mod} p)$

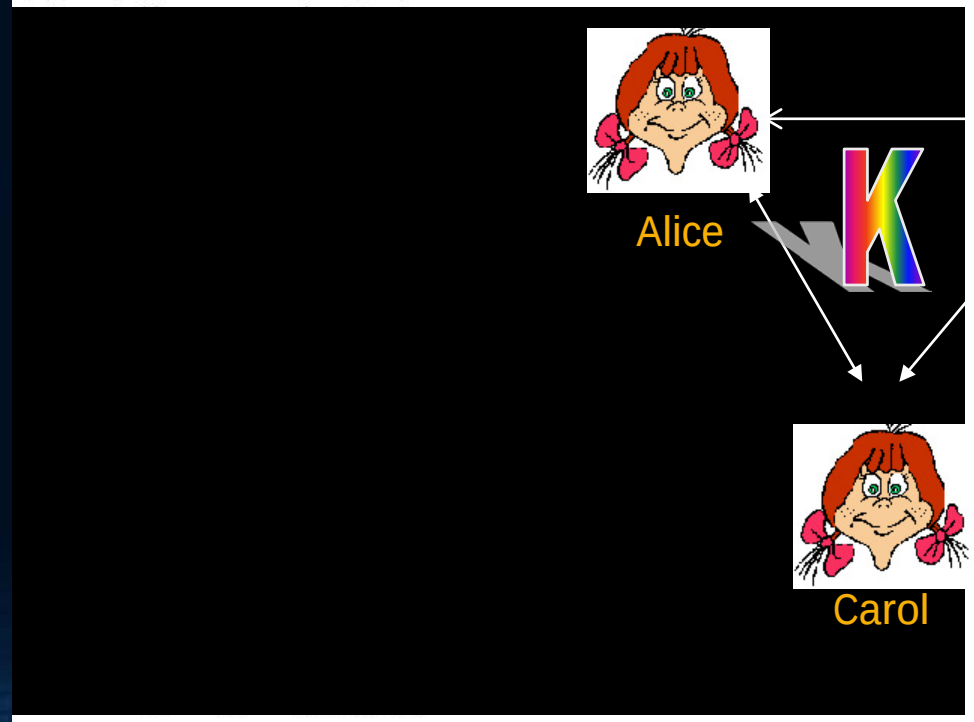
Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Το Πρωτόκολλο Diffie-Hellman

Group Key Agreement

- Πώς μπορούν 3 ή περισσότεροι χρήστες να συμφωνήσουν σε ένα κοινό κλειδί K …
- … Χρησιμοποιώντας το πρωτόκολλο DH;

(1) Alice chooses a random large integer x and sends Bob
$X = g^x \bmod n$
(2) Bob chooses a random large integer y and sends Carol
$Y = g^y \bmod n$
(3) Carol chooses a random large integer z and sends Alice
$Z = g^z \bmod n$



Group Key Agreement

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Το Πρωτόκολλο Diffie-Hellman

Group Key Agreement

- Πώς μπορούν 3 ή περισσότεροι χρήστες να συμφωνήσουν σε ένα κοινό κλειδί K …
- … Χρησιμοποιώντας το πρωτόκολλο DH;

Group Key Agreement

(1) Alice chooses a random large integer x and sends Bob

$$X = g^x \bmod n$$

(2) Bob chooses a random large integer y and sends Carol

$$Y = g^y \bmod n$$

(3) Carol chooses a random large integer z and sends Alice

$$Z = g^z \bmod n$$

(4) Alice sends Bob

$$Z' = Z^x \bmod n$$

(5) Bob sends Carol

$$X' = X^y \bmod n$$

(6) Carol sends Alice

$$Y' = Y^z \bmod n$$

(7) Alice computes

$$k = Y'^x \bmod n$$

(8) Bob computes

$$k = Z'^y \bmod n$$

(9) Carol computes

$$k = X'^z \bmod n$$

Alice

Bob

Carol

Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

Αλγόριθμοι Δημόσιου Κλειδιού

Το «όραμα» των Diffie - Hellman

- Κάθε χρήστης διαθέτει:
  1. ένα Ιδιωτικό (ΙΚ) Κλειδί d_B
  2. ένα Δημόσιο (ΔΚ) Κλειδί e_B

Δεν απαιτείται μυστικότητα κατά την κρυπτογράφηση !!

- Χρήση μονόδρομων συναρτήσεων κρυφής εισόδου (trapdoor one-way)
  - Εύκολη η κρυπτογράφηση,
  - Δύσκολη η αποκρυπτογράφηση, εκτός και αν έχεις τη μυστική πληροφορία

Έχοντας το ένα κλειδί, είναι «δύσκολο» να βρεθεί το άλλο

- Τα κλειδιά μπορούν να χρησιμοποιηθούν για:
  1. Κρυπτογράφηση (encryption)
     - Κρυπτογράφηση με το ΔΚ,
     - Αποκρυπτογράφηση με το ΙΚ
  2. Ψηφιακή υπογραφή (digital signature)
     - Κρυπτογράφηση (υπογραφή) με ΙΚ
     - Επαλήθευση με ΔΚ
  3. Εδραίωση συμμετρικού κλειδιού σε μη ασφαλή περιβάλλοντα

Ασύμμετρα Κρυπτοσυστήματα

Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

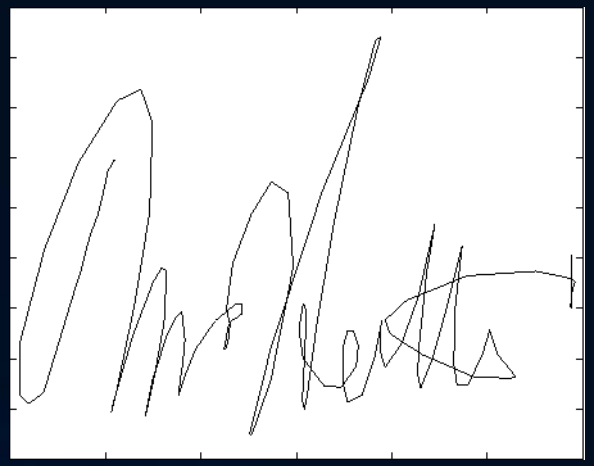
Αλγόριθμοι Δημόσιου Κλειδιού

Δημοφιλείς Αλγόριθμοι

Αλγόριθμοι:

- Κρυπτογράφησης & Ψηφιακής Υπογραφής
  - RSA, ElGamal, Rabin,…
- Ψηφιακής Υπογραφής (αποκλειστικά)
  - Digital Secure Algorithm (DSA),…
    - 1991: NIST- Πρότυπο DSS (Digital Signature Standard)
- Κρυπτογράφησης (αποκλειστικά)
  - Paillier, Goldwasser-Micali,…
- Εδραίωσης Κλειδιών (Key Establishment) ή/και Ταυτοποίησης (Identification)
  - Diffie-Hellmann, S/Key, EKE, …

Καταβολές: στον αλγόριθμο ElGamal



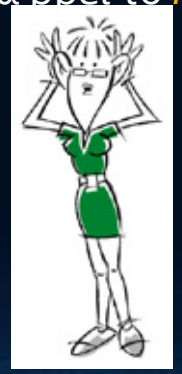
J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Αλγόριθμοι Δημόσιου Κλειδιού

Απόλυτη Ασφάλεια (Perfect Secrecy)

- Σε αντίθεση με τα συμμετρικά συστήματα, στα συστήματα ΔΚ η απόλυτη ασφάλεια δεν είναι εφικτή
  - Δεδομένου ενός ΔΚ pk και ενός κρυπτογραφήματος $c \leftarrow \mathrm{Enc}_{pk}(m)$
  - … ένας εχθρός με άπειρους υπολ. πόρους (unbounded) θα βρει το m με πιθανότητα 1.

… π.χ. δοκιμάζοντας κάθε πιθανό ιδιωτικό κλειδί μέχρι να βρει το σωστό



Problem
FACTORING
RSAP
SQROOT
DLP
DHP

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2001

Κρυπτογραφία Δημόσιου Κλειδιού
Ο αλγόριθμος RSA

Ο αλγόριθμος RSA

1. Η Alice επιλέγει τυχαία δύο πρώτους αριθμούς p, q ϵ Z^*_N
2. Η Alice υπολογίζει N = p * q
3. Η Alice διαλέγει αριθμό e ϵ $Z^*_{\Phi(N)}$
4. Η Alice υπολογίζει αριθμό d ϵ Z_N^*, ώστε $e * d \equiv 1 \pmod{\phi(N)}$
5. Η Alice διαγράφει τα p και q

- Δημόσιο Κλειδί : (e, N)
- Ιδιωτικό Κλειδί : d

- Έστω αριθμός $m \in Z_N^*$
  - Κρυπτογράφηση: $m^e \bmod n \Rightarrow c$
  - Αποκρυπτογράφηση: $c^d \bmod n \Rightarrow m$

(Υπολογιστική) Ασφάλεια

- RSA problem. Ανάγεται στο:
- Factoring problem: Πρόβλημα εύρεσης πρώτων παραγόντων μεγάλων αριθμών
  - Για μεγάλο N, (>= 1024 bit), «δύσκολο» να βρεθούν οι πρώτοι παράγοντες p και q
    - Υπολογιστικά Αδύνατο

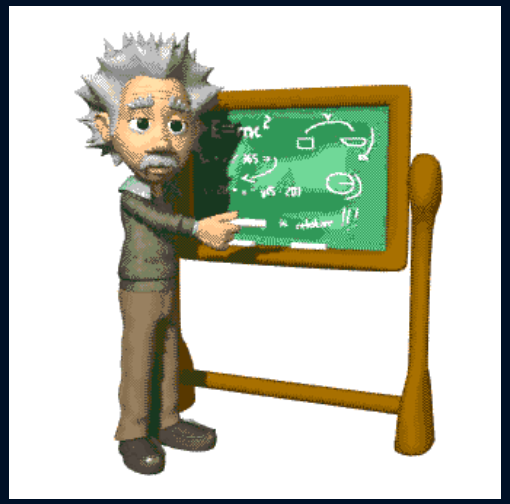
J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Κρυπτογραφία Δημόσιου Κλειδιού
Ο αλγόριθμος RSA

RSA Problem

Δίνονται: Ακέραιος N, θετικός ακέραιος e σχετικά πρώτος με $\Phi(N)$, και ένα στοιχείο y ε Z^*_N.

Υπολόγισε: έναν αριθμό x ώστε $x^e = y \bmod N$



- Ας δούμε την Ασυμμετρία
  - Έστω η ομάδα Z^*_N.
  - Αν η παραγοντοποίηση του N είναι γνωστή τότε το RSA problem γίνεται εύκολο:
    1. Υπολόγισε $\Phi(N)=(p-1)(q-1)$
    2. Υπολόγισε $d = e^{-1} \bmod \Phi(N)$
    3. Υπολόγισε $x = y^d \bmod N$

Κρυφή είσοδος (trapdoor):
οι αριθμοί p, q

H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2001

Κρυπτογραφία Δημόσιου Κλειδιού

Ο αλγόριθμος RSA

- Βήμα 1 Επιλέγουμε τυχαία δύο μεγάλους πρώτους αριθμούς p και q.
- Βήμα 2. Υπολογίζουμε το n = pq και ϕ = (p – 1)(q – 1).
- Βήμα 3 Επιλέγουμε έναν αριθμό e τέτοιο ώστε gcd(e, ϕ) = 1.
- Βήμα 4 Βρίσκουμε τον πολλαπλαστιαστικό αντίστροφο παράγοντα του ϕ, π.χ., ed ≡ 1 (mod ϕ).

Αυτό μπορεί να ανευρεθεί από τον επεκταμένο αλγόριθμο του ευκλείδη

- Το ΔΚ κρυπτογράφησης είναι KE = (n, e) και το ιδιωτικό κλειδί αποκρυπτογράφησης είναι KD = (n, d).
- Η συνάρτηση κρυπτογράφησης είναι E(M) =$M^e mod n$.
- και η συνάρτηση αποκρυπογράφησης D(M) = $M^d mod n$.

D(E(M)) = M και E(D(M)) = M για κάθε o ≤ M < n.

1. Ας δούμε ένα αριθμητικό παράδειγμα. ¨1. Έστω p = 7 και q = 13 είναι οι δύο πρώτοι ➔. n = pq = 91 και ϕ = (p - 1) (q - 1) = 72.

2. Επιλέξτε ε. Ας δούμε ανάμεσα στους πρώτους.

3. Ας βρούμε d. Θέλουμε να βρούμε d τέτοιο ώστε ed ≡ 1 (mod ϕ) το οποίο είναι ισοδύναμο για να βρείτε δ τέτοιο ώστε ed + 1 = ϕk για κάποιον ακέραιο k. Υπενθυμίζουμε ότι gcd (e, ϕ) = 1.

4. Μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο του Ευκλείδη Επέκταση στα βρείτε ακεραίων x και y τέτοια ώστε

ex + ϕy = gcd (e, ϕ). Εάν ε = 5 και ϕ = 72, βρίσκουμε x = 29 και y = -2.

Πράγματι, 5 (29) + 72 (-2) = gcd (5, 72) = 1. Στην συνέχεια, d = 29. Σε γενικές γραμμές, χρησιμοποιούμε d = x mod ϕ.

5. Η λειτουργία κρυπτογράφησης είναι E (M) = M^e mod n = M^5 mod 91. Η συνάρτηση αποκρυπτογράφησης είναι

- D (M) = M^d mod n = M^{29} mod 91.

6. . Ας υποθέσουμε ότι το μήνυμα είναι M = 10.

- E (M) = E (10) = 10^5 mod 91 = 82
- D (E (M)) = D (82) = 82^{29} mod 91 = 10

Ας δούμε πώς μπορείτε να υπολογίσετε αποτελεσματικά 82^{29} mod 91 χρησιμοποιώντας την τετραγωνική-και-πολλαπλασιάζονται αλγόριθμο.

- Δοκιμάστε e = 2. gcd (2, 72) = 2 (δεν λειτουργεί)
- Δοκιμάστε e = 3. gcd (3, 72) = 3 (δεν λειτουργεί)
- Δοκιμάστε e = 5. gcd (5, 72) = 1 (λειτουργεί)

Επιλέγουμε e = 5.

$(82)^1 \equiv 82 \pmod{91}$
$(82)^2 \equiv 81 \pmod{91}$
$(82)^4 \equiv (81)^2 \equiv 9 \pmod{91}$
$(82)^8 \equiv (9)^2 \equiv 81 \pmod{91}$
$(82)^{16} \equiv (81)^2 \equiv 9 \pmod{91}$
Από 29 = 16 + 8 + 4 + 1 (στο δυαδικό είναι 29 11101), συμπεραίνουμε ότι
$82^{29} \equiv (82)^{16} (82)^8 (82)^4 (82)^1 \pmod{91}$
$\equiv (9)(81)(9)(82) \pmod{91}$
$\equiv 10 \pmod{91}$
Καταλήγουμε στο συμπέρασμα ότι 82^{29} mod 91 = 10.

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Οι πρώτοι p και q μπορούν να χρησιμοποιηθούν για να «επιταχυνθούν» οι διεργασίες στον παραλήπτη

Κρυπτογραφία Δημόσιου Κλειδ
Ο αλγόριθμος RSA – Αποδοτικοί Υπολογισμοί

Example 10.16

Say $p = 11$, $q = 23$, and $e = 3$. Then $N = 253$, $\phi(N) = 220$, and $d = 147$.

To encrypt the binary message $m = 0111001$ with textbook RSA and the public key $pk = \langle N = 253, e = 3 \rangle$, simply interpret m as the number 57 (and hence an element of $\mathbb{Z}^*_{253}$) in the natural way. Then compute

$$250 := [57^3 \bmod 253].$$

To decrypt, compute $57 := [250^{147} \bmod 253]$. Alternatively, using the Chinese remainder theorem the receiver could compute

$$250^{[147 \bmod 10]} \bmod 11 = 8^7 \bmod 11 = 2$$

and

$$250^{[147 \bmod 22]} \bmod 23 = 20^{15} \bmod 23 = 11.$$

Indeed, $57 \leftrightarrow (2, 11)$ and so decryption succeeds. (The desired answer can be recovered from the representation $(2, 11)$ as described in Section 7.1.5.) ♢

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμοι Δημόσιου Κλειδιού

Ο αλγόριθμος Rabin

Algorithm Rabin public-key encryption

SUMMARY: B encrypts a message m for A, which A decrypts.

1. *Encryption.* B should do the following:
   (a) Obtain A's authentic public key n.
   (b) Represent the message as an integer m in the range $\{0, 1, \ldots, n-1\}$.
   (c) Compute $c = m^2 \bmod n$.
   (d) Send the ciphertext c to A.
2. *Decryption.* To recover plaintext m from c, A should do the following:
   (a) Use Algorithm 3.44 to find the four square roots m_1, m_2, m_3, and m_4 of c modulo n.[2] (See also Note 8.12.)
   (b) The message sent was either m_1, m_2, m_3, or m_4. A somehow (cf. Note 8.14) decides which of these is m.

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμοι Δημόσιου Κλειδιού

Ο αλγόριθμος Rabin -Παράδειγμα

- Δημιουργία Κλειδιού: η Alice επιλέγει δύο πρώτους p=277, q=331, και υπολογίζει n = p x q = 91687. Το ΔΚ της Alice είναι το n =91687, ενώ το ΙΚ είναι το (p = 277 and q = 331)

- Κρυπτογράφηση:

  1. η Alice και ο Bob συμφωνούν σε κάποια bit πλεονασμού για το μήνυμα που θα σταλεί (π.χ. **100011**)
  2. Ο Bob κρυπτογραφεί το μήνυμα 1001111001 ως εξής:

m=1000111001111001 → m=40569

$C = m^2 \bmod n = 40569^2 \bmod 91687 = 62111$

- Αποκρυπτογράφηση: η Alice βρίσκει τις τετραγωνικές ρίζες του C, modulo n
  - Εύκολο: βρίσκει 2 ρίζες modulo p και 2 ρίζες modulo q:

m_1=69954, m_2=22033,
m_3=40569, m_4=45118

m1=1000100000010110,
m2=101011000010001,
m3=1001111001111001,
m4=110001111010110.

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Αλγόριθμοι Δημόσιου Κλειδιού

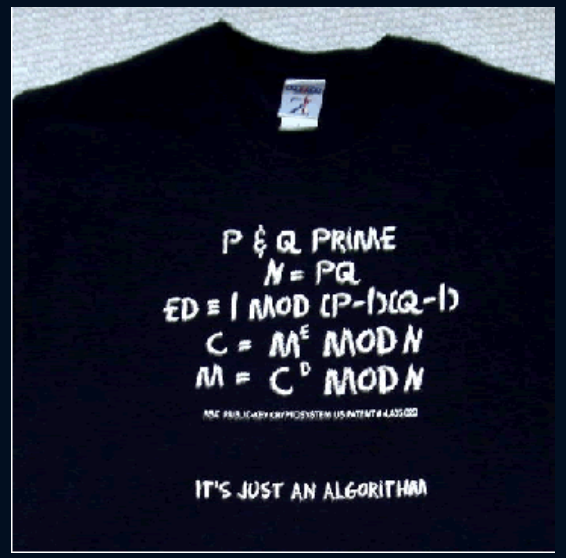
Ντετερμινιστικοί και Πιθανοτικοί Αλγόριθμοι

- Τα ντετερμινιστικά σχήματα ΔΚ (π.χ. RSA, Rabin) δεν είναι ασφαλή
  1. Απλές Κρυπταναλυτικές επιθέσεις

<u>Περίπτωση Κρυπτανάλυσης:</u>
Η Eve ξέρει πότε στέλνεται το ίδιο μήνυμα δύο φορές !!

<u>Περίπτωση:</u> Το κρυπτογράφημα c περιέχει τη βαθμολογία πτυχίου του Bob. Η Eve υποκλέπτει και δοκιμάζει πιθανές τιμές στο [1..10]

  2. Ασφάλεια από επιθέσεις CPA, CCA (Chosen Plaintext/Ciphertext)



<u>Λύσεις</u>

1. «Διόρθωση» παραδοσιακών κρυπτοσυστημάτων
   - π.χ. OAEP RSA (PKCS #1 v2.1)
2. Χρήση πιθανοτικών αλγορίθμων
   - π.χ. ElGamal-like

RSA Επιθέσεις

- Όταν η κρυπτογράφηση γίνεται με μικρούς εκθέτες (π.χ., $e = 3$), και μικρές τιμές του m, *(δηλ,* $m < n^{1/e}$) το αποτέλεσμα του m^e μικρότερο από το N. Σε αυτή την περίπτωση, τα ciphertexts μπορεί εύκολα να αποκρυπτογραφηθούν χρησιμοποιώντας την $\sqrt[e]{chiphertext}$ modN.

- Εάν το ίδιο μήνυμα κειμένου στέλνεται *στο* e ή περισσότερους παραλήπτες, και οι δέκτες μοιράζονται τον ίδιο εκθέτη *e*, αλλά διαφορετικές *p*, *q*, και ως εκ τούτου *το N*, τότε είναι εύκολο να αποκρυπτογραφήσει το αρχικό μήνυμα μέσω του Κινέζικο Θεώρημα Υπολοίπων. Αυτή η επίθεση είναι δυνατή ακόμη και αν τα cleartexts δεν είναι ίδια, αλλά ο επιτιθέμενος γνωρίζει μια γραμμική σχέση μεταξύ τους. Αυτή η επίθεση έγινε αργότερα βελτιώθηκε από τον Don Coppersmith.

- Επειδή η κρυπτογράφηση RSA είναι ένας ντετερμινιστικός αλγόριθμος κρυπτογράφησης (δηλαδή, δεν έχει τυχαία συνιστώσα) ένας εισβολέας μπορεί να ξεκινήσει με επιτυχία μια chosen plaintext επίθεση εναντίον του κρυπτοσυστήματος, με την χρήση κρυπτογραφημένων πιθανών plaintexts κάτω από το δημόσιο κλειδί και δοκιμής, εάν αυτές είναι ίσες με το κρυπτογράφημα. Ένα κρυπτογραφικό σύστημα λέγεται σημασιολογικά ασφαλής αν ένας εισβολέας δεν μπορεί να διακρίνει δύο κρυπτογραφήσεις, ακόμη και αν ο επιτιθέμενος γνωρίζει τα plaintexts. Ο RSA δεν είναι σημασιολογικά ασφαλής. [

- Στον RSA το γινόμενο δύο κρυπτοκειμένων είναι ίση με την κρυπτογράφηση των αντίστοιχων plaintexts. Δηλαδή $m_1^e m_2^e \equiv (m_1 m_2)^e \pmod{n}$. Λόγω αυτής της πολλαπλασιαστικής ιδιοτητας μια chosen plaintext επίθεση είναι εφικτή. Π.χ., ένας εισβολέας, ο οποίος θέλει να ξέρει την αποκρυπτογράφηση του ciphertext $c \equiv m^e \pmod{n}$ μπορεί να ζητήσει από τον κάτοχο του ιδιωτικού κλειδίου την αποκρυπτογράφηση του $c' \equiv cr^e \pmod{n}$ για κάποιο r που επιλέγεται από τον εισβολέα. Λόγω της πολλαπλασιαστικής ιδιότητας το c 'είναι η κρυπτογράφηση του $mr \pmod{n}$. Ως εκ τούτου, εάν ο επιτιθέμενος μάθει *το* $mr \pmod{n}$ μπορεί να ανακαλήψει το μήνυμα m από τον πολλαπλασιασμό *του mr* με την αντίστροφη *του r modulo* n.

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Αλγόριθμοι Δημόσιου Κλειδιού

The padded RSA

CONSTRUCTION 10.18

Let GenRSA be as before, and let ℓ be a function with $\ell(n) \leq 2n - 2$ for all n. Define a public-key encryption scheme as follows:

- Gen: on input 1^n, run GenRSA(1^n) to obtain (N, e, d). Output the public key $pk = \langle N, e \rangle$, and the private key $sk = \langle N, d \rangle$.
- Enc: on input a public key $pk = \langle N, e \rangle$ and a message $m \in \{0,1\}^{\ell(n)}$, choose a random string $r \leftarrow \{0,1\}^{\|N\| - \ell(n) - 1}$ and interpret $r \| m$ as an element of $\mathbb{Z}_N$ in the natural way. Output the ciphertext
$$c := [(r\|m)^e \bmod N].$$
- Dec: on input a private key $sk = \langle N, d \rangle$ and a ciphertext $c \in \mathbb{Z}_N^*$, compute
$$\hat{m} := [c^d \bmod N],$$
and output the $\ell(n)$ low-order bits of $\hat{m}$.

The padded RSA encryption scheme.

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Αλγόριθμοι Δημόσιου Κλειδιού

CPA-secure RSA

CONSTRUCTION 13.1

Let GenRSA be as usual, and let $\ell(n)$ be an arbitrary polynomial. Let H be a function whose domain can be set to $\mathbb{Z}_N^*$ for any N, and whose range can be set to $\{0,1\}^{\ell(n)}$ for any n. Construct a public-key encryption scheme as follows:

- Gen: on input 1^n, run GenRSA(1^n) to compute (N, e, d). The public key is $\langle N, e\rangle$ and the private key is $\langle N, d\rangle$.
- Enc: on input a public key $\langle N, e\rangle$ and a message $m \in \{0,1\}^{\ell(n)}$, choose a random $r \leftarrow \mathbb{Z}_N^*$ and output the ciphertext

$$\langle [r^e \bmod N],\ H(r) \oplus m \rangle .$$

- Dec: on input a private key $\langle N, d\rangle$ and a ciphertext $\langle c_1, c_2\rangle$, compute $r := [c_1^d \bmod N]$ and then output the message $H(r) \oplus c_2$.

CPA-secure RSA encryption in the random oracle model.

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Αλγόριθμοι Δημόσιου Κλειδιού

Ντετερμινιστικοί και Πιθανοτικοί Αλγόριθμοι

CONSTRUCTION 13.5

Let GenRSA be as in the previous section, let $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ be a private-key encryption scheme for messages of length $\ell(n)$, and let H be a function whose domain can be set to $\mathbb{Z}_N^*$ for any N, and whose range can be set to $\{0,1\}^n$ for any n. Construct a public-key encryption scheme as follows:

- Gen: on input 1^n, run $\mathsf{GenRSA}(1^n)$ to compute (N, e, d). The public key is $\langle N, e \rangle$ and the private key is $\langle N, d \rangle$.
- Enc: on input a public key $\langle N, e \rangle$ and a message $m \in \{0,1\}^{\ell(n)}$, choose a random $r \leftarrow \mathbb{Z}_N^*$ and compute $k := H(r)$. Output the ciphertext

$$\langle [r^e \bmod N],\ \mathsf{Enc}'_k(m) \rangle .$$

- Dec: on input a private key $\langle N, d \rangle$ and a ciphertext $\langle c_1, c_2 \rangle$, compute $r := [c_1^d \bmod N]$ and set $k := H(r)$. Then output $\mathsf{Dec}'_k(c_2)$.

CCA-secure RSA encryption in the random oracle model.

Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

Αλγόριθμοι Δημόσιου Κλειδιού

Ο αλγόριθμος ElGamal (1/3)

Algorithm 8.3: The ElGamal Cryptosystem

Key Setup

To set up a user's key material, user Alice performs the following steps:

1. choose a random prime number p;
2. compute a random multiplicative generator element g of $\mathbb{F}_p^*$;
3. pick a random number $x \in_U \mathbb{Z}_{p-1}$ as her private key;
4. compute her public key by

$$y \leftarrow g^x \pmod{p};$$

5. publicize (p, g, y) as her public key, and keep x as her private key.

(* similar to the case of the Diffie-Hellman key exchange protocol, a system-wide users may share the common public parameters (p, g). *)

Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

Αλγόριθμοι Δημόσιου Κλειδιού

Ο αλγόριθμος ElGamal (2/3)

Encryption

To send a confidential message $m < p$ to Alice, the sender Bob picks $k \in_U \mathbb{Z}_{p-1}$ and computes ciphertext pair (c_1, c_2) as follows:

Equation 8.12.1

$$\begin{cases} c_1 \leftarrow g^k \pmod{p}, \\ c_2 \leftarrow y^k m \pmod{p}. \end{cases}$$

Decryption

To decrypt ciphertext (c_1, c_2), Alice computes

Equation 8.12.2

$$m \leftarrow c_2 / c_1^x \pmod{p}.$$

(Υπολογιστική) Ασφάλεια

- Πρόβλημα: Δεδομένων των: p, g, g^x, g^k, $g^{kx} \cdot m$, βρες το m
  - Ισοδύναμο με DHP
  - Ανάγεται στο DLP
- Σημαντικό: Χρήση διαφορετικού k σε κάθε κρυπτογράφηση !

Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

Αλγόριθμοι Δημόσιου Κλειδιού

Ο αλγόριθμος El Gamal

From Example 8.1 we know that 3 is a primitive root modulo 43. Let Alice choose 7 as her private key. She computes her public key as

$$37 \equiv 3^7 \pmod{43}.$$

Alice publicizes her public key material $(p, g, y) = (43, 3, 37)$.

Let Bob encrypt a plaintext message $m = 14$. Bob picks a random exponent 26 and computes

$$c_1 = 15 \equiv 3^{26} \pmod{43}, \quad c_2 = 31 \equiv 37^{26} \times 14 \pmod{43}.$$

The resultant ciphertext message pair is (15, 31).

To decrypt the ciphertext message (15, 31), Alice computes

$$14 = 31/36 \equiv 31/15^7 \pmod{43}.$$

Division requires application of Alg 4.2. But Alice can avoid it by computing:

$$14 = 31 \times 15^{42-7} \equiv 31 \times 6 \pmod{43}.$$

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Αλγόριθμοι Δημόσιου Κλειδι

Ο αλγόριθμος Goldwasser-Micali

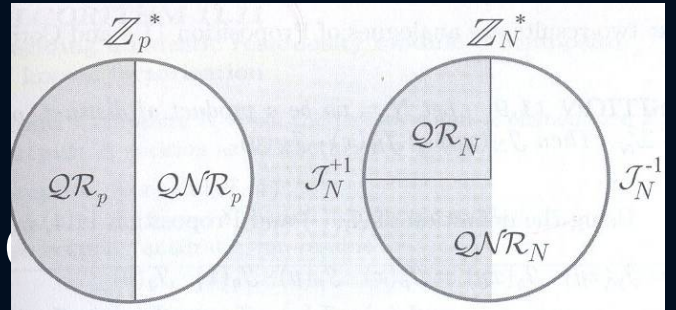


FIGURE 11.1: The structure of $\mathbb{Z}_p^*$ and $\mathbb{Z}_N^*$.

CONSTRUCTION 11.13

Let GenModulus be a polynomial-time algorithm that, on input 1^n, outputs (N, p, q) where $N = pq$, and p and q are n-bit primes except with probability negligible in n. Construct a public-key encryption scheme as follows:

- Gen: on input 1^n, run GenModulus(1^n) to obtain (N, p, q), and choose a random $z \leftarrow \mathcal{QNR}_N^{+1}$. The public key is $pk = \langle N, z \rangle$ and the private key is $sk = \langle p, q \rangle$.
- Enc: on input a public key $pk = \langle N, z \rangle$ and a message $m \in \{0, 1\}$, choose a random $x \leftarrow \mathbb{Z}_N^*$ and output the ciphertext

$$c := [z^m \cdot x^2 \bmod N].$$

- Dec: on input a private key $sk = \langle p, q \rangle$ and a ciphertext c, determine whether c is a quadratic residue modulo N using, e.g., Algorithm 11.11. If c is a quadratic residue, output 0; otherwise, output 1.

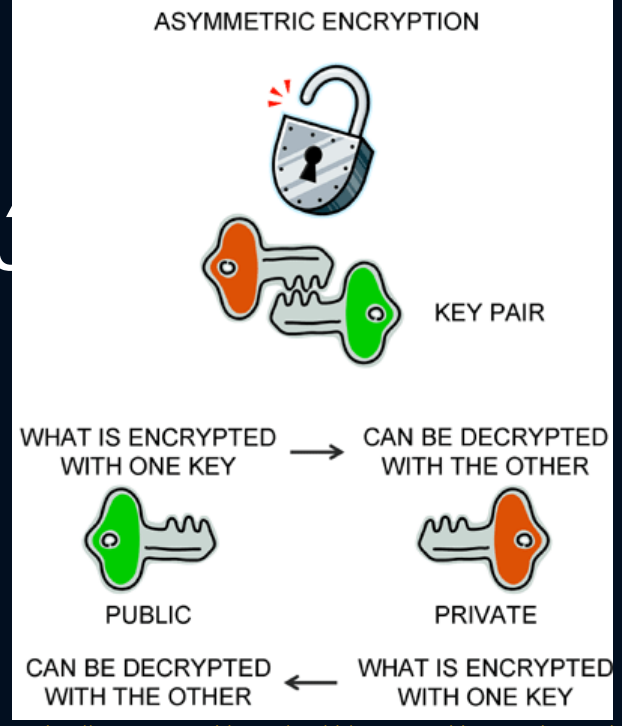
The Goldwasser-Micali encryption scheme.

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Αλγόριθμοι Δημοσίου Κλειδιού

Συνοπτικά

A. Κρυπτογράφησης
   1. Factoring problem
      - RSA (RSA problem)
      - Rabin (Square Root)
      - Goldwasser-Micali (Quadratic Residuosity)
      - Paillier
   2. Discrete Log Problem
      - Diffie-Helmann (DDH)
      - ElGamal (DDH)



http://www.teracom-training.com/tutorials/teracom-tutorial-asymmetric-encryption.gif

B. Ψηφιακής Υπογραφής
   1. Factoring problem
      - RSA, Rabin
   2. Discrete Log Problem
      - ElGamal, Schnorr,
      - DSA (DSS)
   - …

Σύγκριση και Επιλογή Αλγορίθμων...

Συμμετρικοί Αλγόριθμοι και Αλγόριθμοι Δημόσιου Κλειδιού

H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2000

Encryption or MAC

Encryption or signature

Assurance	Prevents	Secret Key	Public Key
Confidentiality	Snooping	x	x
Authentication	Masquerading	x	x
Integrity	Message alteration without detection	x	x
Nonrepudiation	Sender's false denial		x

Algorithm	Confidentiality	Authentication	Integrity
Symmetric encryption algorithms	Yes	No	No
Public-key encryption algorithms	Yes	No	No
Digital signature algorithms	No	Yes	Yes
Key-agreement algorithms	Yes	Optional	No
One-way hash functions	No	No	Yes
Message authentication codes	No	Yes	Yes

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2000

Σύγκριση και Επιλογή Αλγορίθμων...

Συμμετ

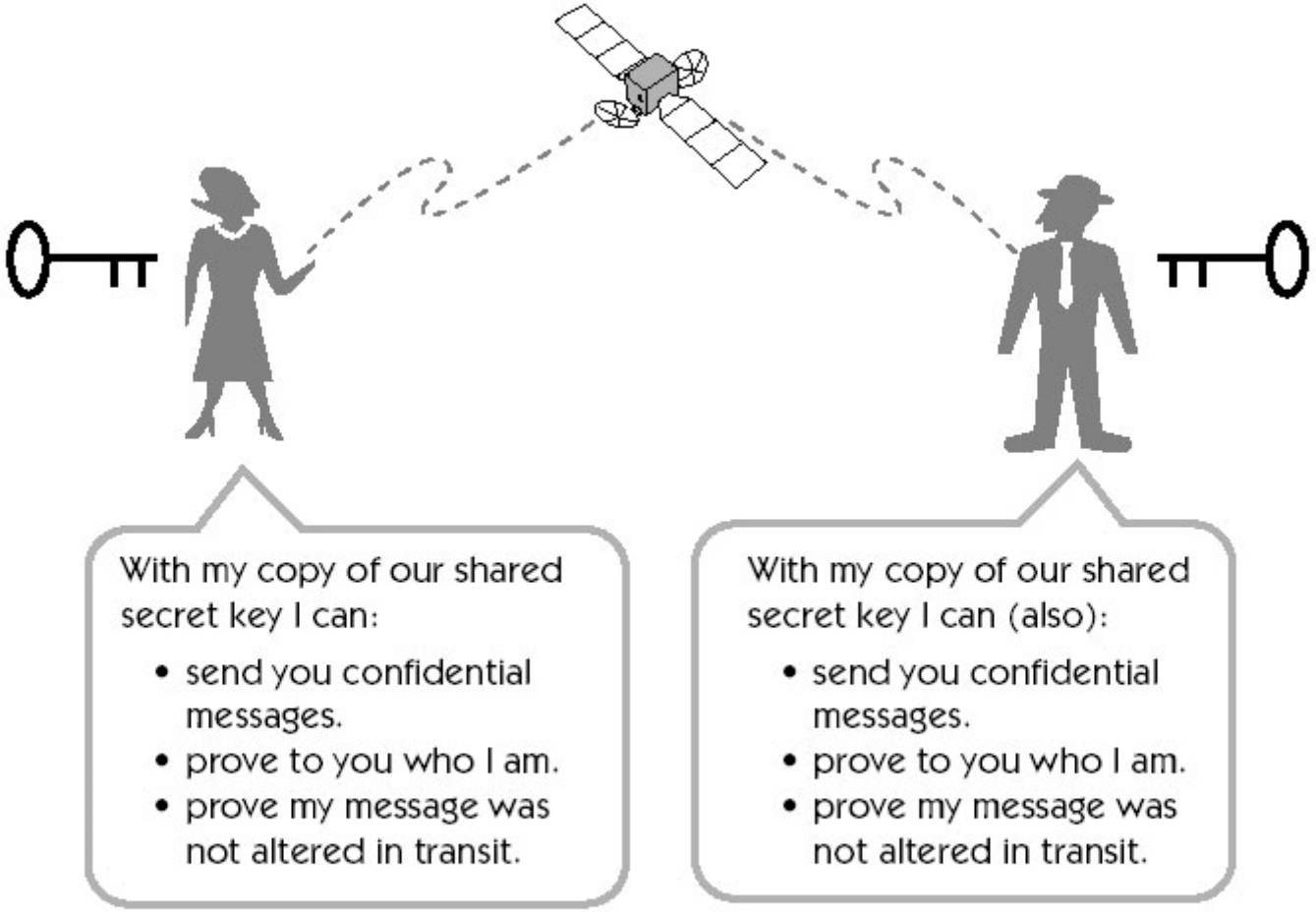


Figure 15-1 In symmetric (secret key) cryptography the holders look symmetric and have identical attributes.

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2000

Σύγκριση και Επιλογή Αλγορίθμων...

Συμμετρικ

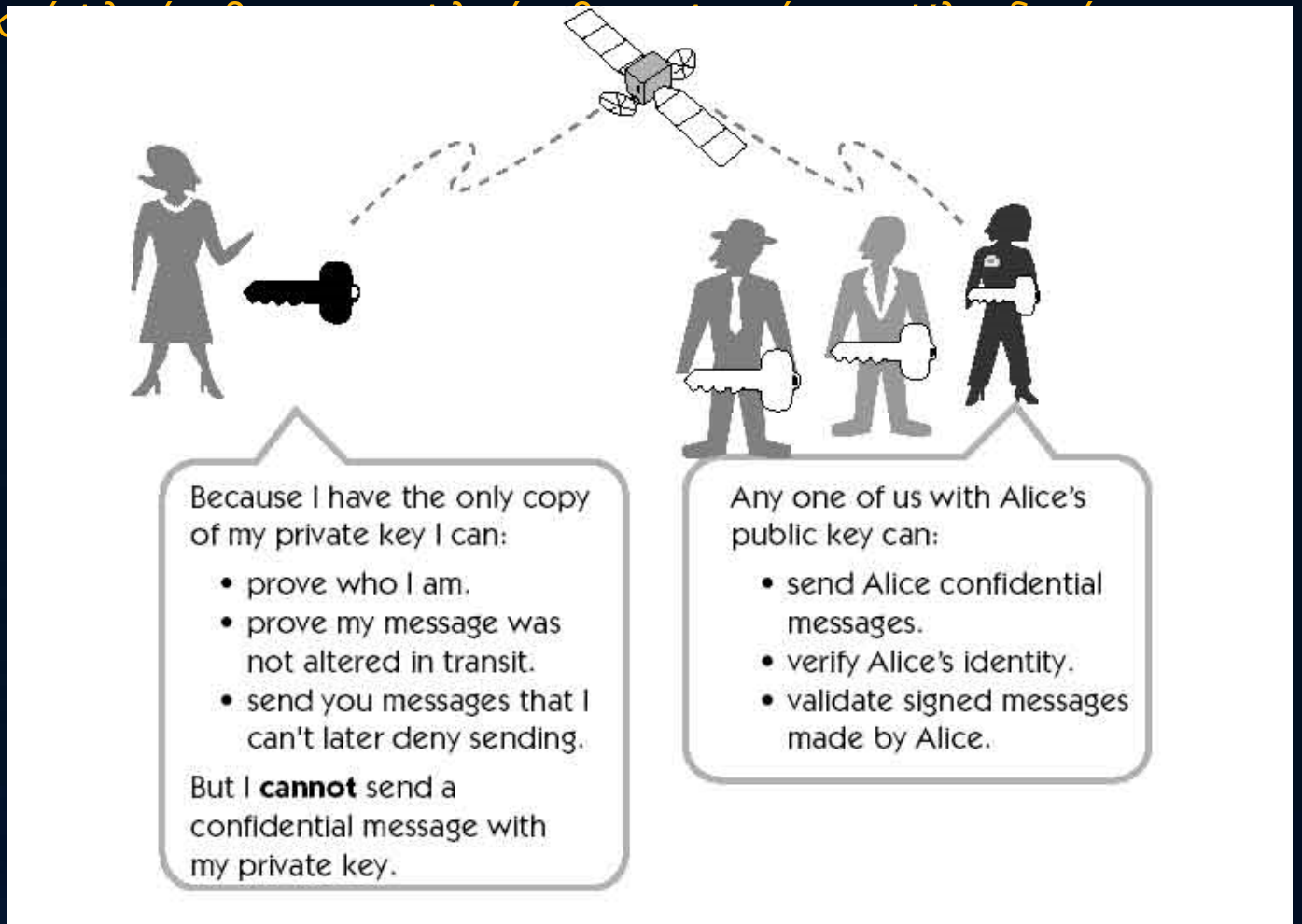


Figure 15-2 In asymmetric (public key) cryptography the holders look different and have different attributes.

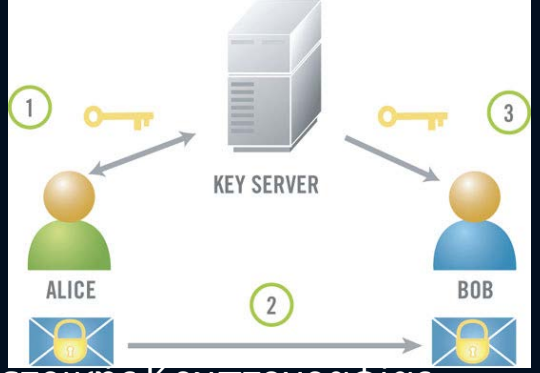
H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2000

Σύγκριση και Επιλογή Αλγορίθμων...

Συμμετρικοί Αλγόριθμοι και Αλγόριθμοι Δημόσιου Κλειδιού

Attribute	Secret Key	Public/Private Key
Years in use	Thousands	Less than 50
Current main use	Bulk data encryption	Key exchange, digital signatures
Current standard	DES, Triple DES, and Rijndael	RSA, Diffie-Hellman, DSA
Encryption / decryption speed	Fast	Slow
Keys	Shared secret between at least two people (usually only two)	Private: kept concealed by one person Public: widely distributed
Key exchange	Difficult and risky to transfer a secret key	Easy and less risky to deliver a public key Private key never shared
Key length	56-bit obsolete 128-bit considered safe	1,024 suggested (RSA) Some users demand 2,048
Confidentiality, authentication, message integrity	Yes	Yes
Nonrepudiation	No Need trusted third party to act as witness	Yes Digital signatures: don't need trusted third party
Attacks	Yes	Yes

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001



Σύγκριση και Επιλογή Αλγορίθμων...

Συμμετρικοί Αλγόριθμοι και *Αλγόριθμοι Δημ. Κλειδιού*

Πλεονεκτήματα Συμμετρικής Κρυπτογραφίας

- Υψηλή απόδοση
  - ιδίως, σε υλοποιήσεις hardware
- Κλειδιά μικρού μήκους
  - π.χ. (128-256) bit
- Ευρεία χρήση στη δημιουργία άλλων κρυπτογραφικών εργαλείων
  - Γεννήτορες (ψευδο-) τυχαιότητας
  - Μονόδρομες συναρτήσεις hash
  - Συναρτήσεις MAC
- Μακρά ιστορία

φάλεια τους έχει «δοκιμαστεί»

Μειονεκτήματα Συμμετρικής Κρυπτογραφίας

- Το κλειδί πρέπει να κρατείται μυστικό από όλους τους συμμετέχοντες (π.χ. Alice, Bob)
- Πλήθος κλειδιών σε δίκτυα μεγάλης κλίμακας
  - Δύσκολη Διαχείριση
  - Αν μια Τρίτη Οντότητα (ΤΟ) «μοιράζει» κλειδιά, τότε οι χρήστες εμπιστεύονται την ΤΟ
- Το κλειδί πρέπει να αλλάζει συχνά
  - Αν είναι δυνατό, σε κάθε σύνοδο (session) μεταξύ δύο χρηστών

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Σύγκριση και Επιλογή Αλγορίθμων...

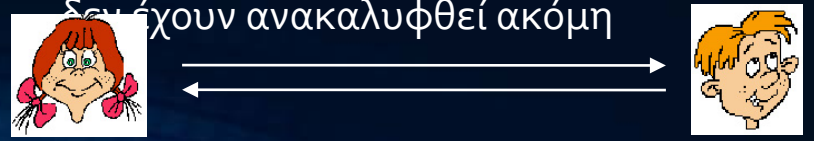
Συμμετρικοί Αλγόριθμοι και *Αλγόριθμοι Δημόσιου Κλειδιού*

Πλεονεκτήματα Κρυπτογραφίας Δ.Κ.

- Μόνον το ιδιωτικό κλειδί πρέπει να περιβάλλεται από μυστικότητα
- Η εμπιστοσύνη σε μια Τρίτη Οντότητα δεν είναι τόσο ισχυρή
  - π.χ Η Τρίτη Οντότητα τηρεί μια ΒΔ με τα ΔΚ των χρηστών
- Μικρό πλήθος κλειδιών
  - π.χ. σε ένα δίκτυο Ν χρηστών, υπάρχουν Ν ζεύγη κλειδιών
- Ένα ζεύγος ΙΚ-ΔΚ μπορεί να έχει μεγάλη διάρκεια ζωής
- Αυθεντικοποίηση σε κρυπτογραφικά πρωτόκολλα
  - Μη Αποποίηση Ευθύνης

Μειονεκτήματα Κρυπτογραφίας Δ. Κ.

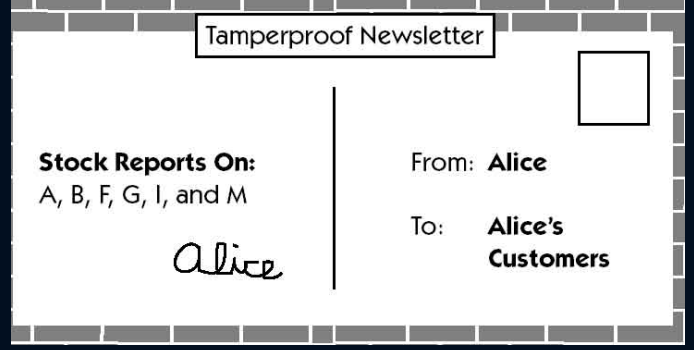
- Χαμηλή απόδοση
  - Έως 1000 φορές πιο «αργές» υλοποιήσεις
- Μεγάλα μήκη κλειδιών
  - π.χ. 2048 bit modulus
- Κανένας αλγόριθμος δεν αποδείχθηκε απόλυτα ασφαλής
  - Σε αντίθεση με το one-time pad
- «Μικρή Ηλικία»
  - Ενδεχομένως, υπάρχουν «τρύπες» που δεν έχουν ανακαλυφθεί ακόμη



Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Ψηφιακή Υπογραφή

- Ασφάλεια φυσικών υπογραφών
  1. Η υπογραφή είναι αυθεντική
     - Ο υπογράφων (και όχι κάποιος άλλος) υπέγραψε το μήνυμα
  2. Η υπογραφή δεν «αποκόβεται»
     - Αποτελεί τμήμα εγγράφου, και δεν μεταφέρεται σε άλλο έγγραφο.
  3. Ακεραιότητα εγγράφου
     - Μετά την υπογραφή, το έγγραφο δεν μπορεί να αλλάξει μορφή
  4. Μη αποποίηση ευθύνης
     - Ο υπογράφων δεν μπορεί να αρνηθεί ότι υπέγραψε το έγγραφο

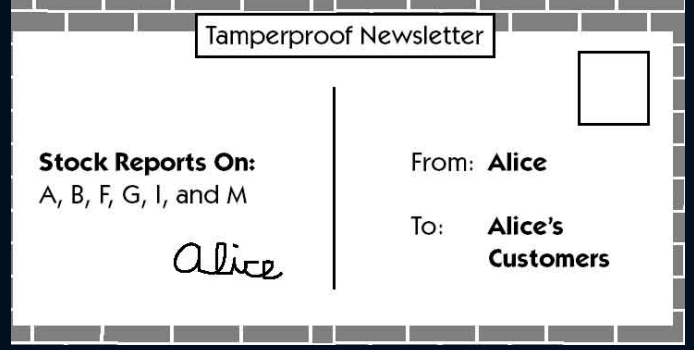


Σκέψεις …

- Εκπληρώνονται οι απαιτήσεις ασφάλειας στον φυσικό κόσμο;
- Πόσο (πιο) δύσκολη η ύπαρξη ασφαλών συστημάτων υπογραφής στο Internet;

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.



Ψηφιακή Υπογραφή

- Ασφάλεια φυσικών υπογραφών
  1. Η υπογραφή είναι αυθεντική
     - Ο υπογράφων (και όχι κάποιος άλλος) υπέγραψε το μήνυμα
  2. Η υπογραφή δεν «αποκόβεται»
     - Αποτελεί τμήμα εγγράφου, και δεν μεταφέρεται σε άλλο έγγραφο.
  3. Ακεραιότητα εγγράφου
     - Μετά την υπογραφή, το έγγραφο δεν μπορεί να αλλάξει μορφή
  4. Μη αποποίηση ευθύνης
     - Ο υπογράφων δεν μπορεί να αρνηθεί ότι υπέγραψε το έγγραφο

- Επιπλέον απαιτήσεις για υπογραφές
  5. Μεταφερσιμότητα
     - π.χ. ο Bob επιδεικνύει ένα ψηφ. πιστοποιητικό στην Carol
  6. Οικουμενική επαληθευσιμότητα
     - π.χ. αποτελέσματα η-εκλογών δημοσιεύονται σε ένα site

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

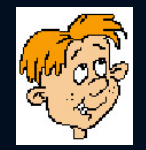
Ψηφιακή Υπογραφή (με Συμμετρική Κρυπτογραφία)

Χρησιμοποιώντας MAC

Setup

- Η Alice και ο Bob έχουν ένα κοινό μυστικό κλειδί K

$M, MAC_K(M)$



Πρωτόκολλο

1. Η Alice υπολογίζει την τιμή MAC, με το κλειδί K, του μηνύματος M και το στέλνει στον Bob
2. Ο Bob επαληθεύει

- Προβλήματα
  - Δύσκολη η Μεταφερσιμότητα
  - Δύσκολη η μη Αποποίηση Ευθύνης
  - Δύσκολη η Οικ. Επαληθευσιμότητα
  - Δύσκολη η Διαχείριση Κλειδιού
    - Ιδίως σε περιβάλλοντα μεγάλης κλίμακας

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Ψηφιακή Υπογραφή (με Συμμετρική Κρυπτογραφία)

Χρήση Τρίτης Έμπιστης Οντότητας

Setup

- Ο Trent και η Alice έχουν ένα κοινό μυστικό κλειδί K_A
- Ο Trent και ο Bob έχουν ένα κοινό μυστικό κλειδί K_B

Όλοι εμπιστεύονται τον Trent !!

Πρωτόκολλο

1. Η Alice κρυπτογραφεί το μήνυμα M με το K_A και το στέλνει στον Trent
2. Ο Trent αποκρυπτογραφεί
3. Ο Trent φτιάχνει ένα μήνυμα που απαρτίζεται από το M, και μια δήλωση ότι το έλαβε από την Alice.
4. Ο Trent κρυπτογραφεί το μήνυμα με το K_B και το στέλνει στον Bob
5. Ο Bob αποκρυπτογραφεί

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

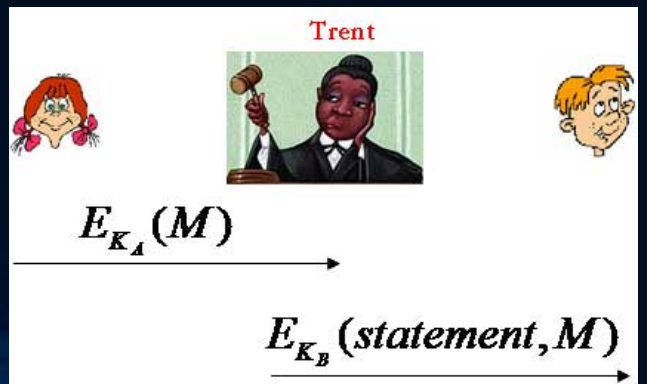
Ψηφιακή Υπογραφή (Συμμετρική Κρυπτογραφία)

Χρήση Τρίτης Έ

Ναι, αν όλοι "εμπιστεύονται" τον Trent

1. Εκπληρώνονται οι απαιτήσεις;

- Αυθεντικότητα
  - Ο Trent την πιστοποιεί…
- Μη Αποκοπή & Ακεραιότητα
  - Ο Bob δε μπορεί να δημιουργήσει μια υπογραφή της Alice χωρίς το K_A
    - Κάθε αλλαγή θα γίνει αντιληπτή από τον Trent.
- Μη Αποποίηση Ευθύνης
  - Ο Trent πιστοποιεί ότι η Alice υπέγραψε το μήνυμα
- Μεταφερσιμότητα
  - Μπορεί ο Bob να δείξει το υπογεγραμμένο έγγραφο στην Carol;
  - Θα εμπλακεί ξανά ο Trent
    - Πρέπει να είναι online,
    - Πρέπει να διατηρεί μια ΒΔ με τα υπογρεγραμμένα μηνύματα
- Οικουμενική Επαληθευσιμότητα
  - Δύσκολη – μη πρακτική



Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Αλγόριθμοι Δημόσιου Κλειδιού

Ψηφιακή Υπογραφή

1. Η Alice και ο Bob συμφωνούν σε ένα κρυπτοσύστημα (π.χ. RSA)

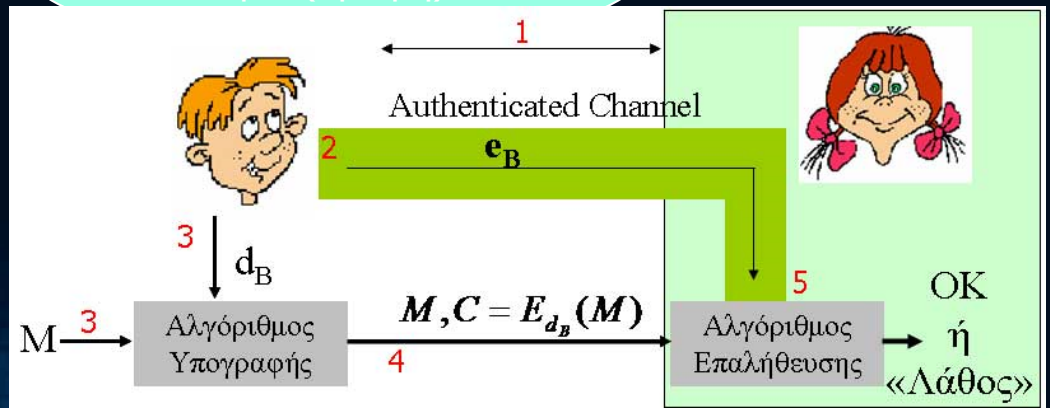
<u>Κρυπτοσύστημα</u> = αλγ/θμος υπογραφής + αλγ/θμος επαλήθευσης

2. Ο Bob στέλνει στην Alice το ΔΚ
3. Ο Bob εισάγει το μήνυμα M και το ιδιωτικό του κλειδί στον αλγόριθμο υπογραφής
   - «Κρυπτογράφηση» με το ΙΚ
4. Ο Bob στέλνει το μήνυμα και τη ψηφιακή υπογραφή στην Alice

- Η Alice εισάγει το μήνυμα, την υπογραφή και το ΔΚ του Bob στον αλγόριθμο επαλήθευσης
  - «Αποκρυπτογράφηση» με το ΔΚ

Ανάγκη για αυθεντικοποίηση

Εναλλακτικά, ανάκτηση από μια (έγκυρη) ΒΔ



Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμοι Δημόσιου Κλειδιού

Ψηφιακή Υπογραφή με τον RSA

ημιουργία Κλειδιών

1. Επιλογή πρώτων:
   - p = 7927, q = 6997
2. Υπολογισμός:
   - n = p * q = 55465219
3. Υπολογισμός:
   - Φ(n) = 7926 * 6996 = 55450296
4. Επιλογή e = 5 και επίλυση της εξίσωσης:
   - 5 * d 1 (mod 55450296)

- Δημόσιο κλειδί:
  - (n = 55465219, e = 5)
- Ιδιωτικό Κλειδί:
  - d = 44360237

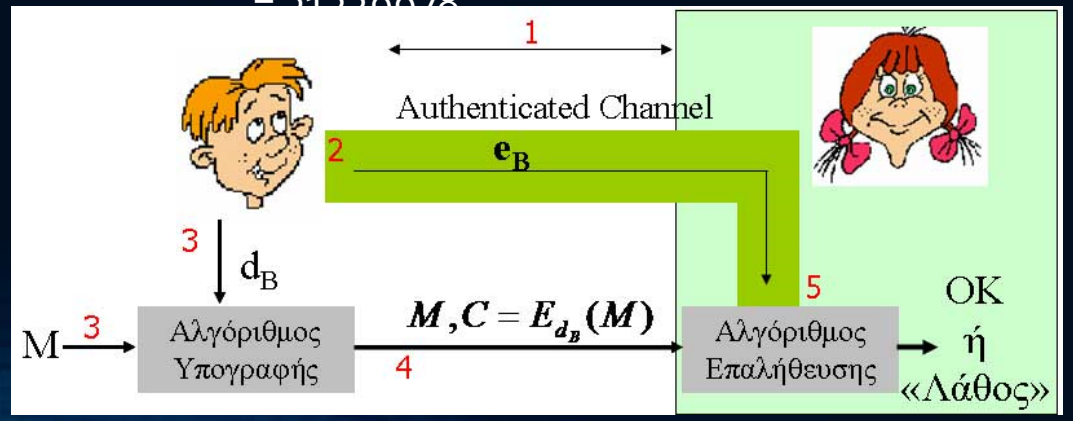
Υπογραφή (του μηνύματος M = 31229978

- C = 31229978 $^{(44360237)}$ mod 55465219

  = 30729435

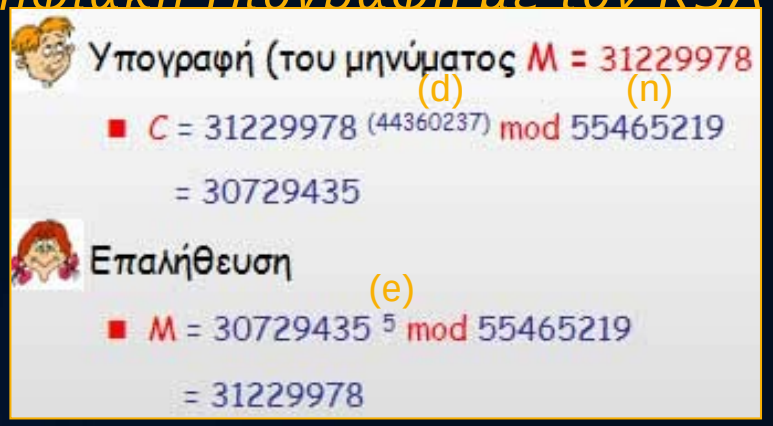
- Επαλήθευση
- M = 30729435 ^{5} mod 55465219

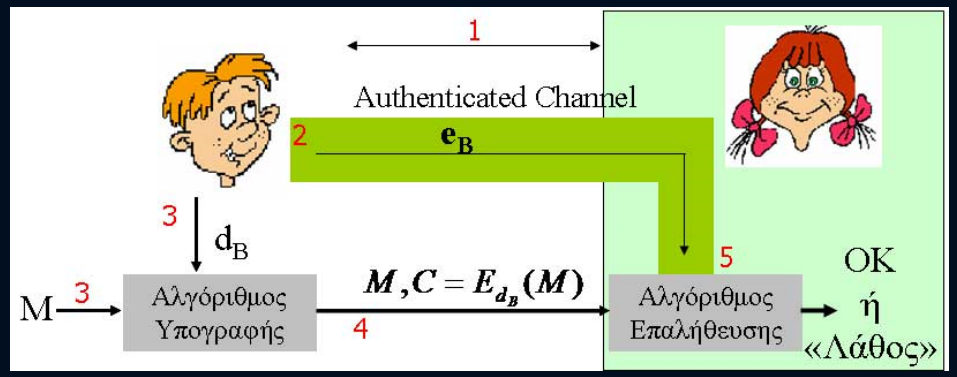
  = 31229978



Αλγόριθμοι Δημόσιου Κλειδιού

Ψηφιακή Υπογραφή με τον RSA





- Αυθεντικότητα
  - Η Alice, εφόσον επαληθεύσει την υπογραφή με το ΔΚ του Bob γνωρίζει ότι αυτός υπέγραψε το M
  - Μόνο ο Bob γνωρίζει το ΙΚ
- Μη Αποκοπή
  - Η υπογραφή «δένεται» με το έγγραφο και δεν μπορεί να μεταφερθεί
- Ακεραιότητα
  - Αν υπάρξει οποιαδήποτε αλλαγή στο έγγραφο, το ΔΚ του Bob δεν θα επαληθεύσει την υπογραφή
- Μη αποποίηση Ευθύνης
  - Όλοι γνωρίζουν ότι ο Bob υπέγραψε το μήνυμα, εφόσον το ΔΚ επαληθεύει την υπογραφή

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Αλγόριθμοι Δημόσιου Κλειδιού

Ψηφιακή Υπογραφή με τον RSA

- Ενδεικτικές επιθέσεις στην "textbook" έκδοση του RSA

1. Existential forgery

Δίνονται: Το δημόσιο κλειδί (N, e).
Πλαστογραφία: Επίλεξε τυχαίο $x \epsilon Z_N^*$ και υπολόγισε $m = x^e \bmod N$.
Εμφάνισε το x ως υπογραφή του m.

2. Malleability

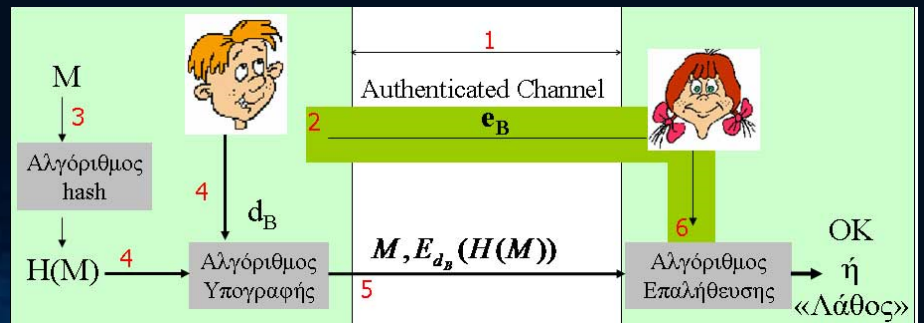
Επίλεξε τυχαίο $m_1 \epsilon Z_N^*$ και υπολόγισε $m_2 = [m/m_1 \bmod N]$. Απόκτησε υπογραφές S_1 και S_2 στα m_1 και m_2. Βρες $S = S_1 * S_2$.
Εμφάνισε το S ως υπογραφή στο m.

- Λύση: Το M εισάγεται σε μια κρυπτογραφική συνάρτηση hash (π.χ. SHA-1) πριν υπογραφεί

a) Οι προηγούμενες επιθέσεις γίνονται "δύσκολες"

b) Η αποδοτικότητα βελτιώνεται

- π.χ. τα μηνύματα "συμπιέζονται" σε μέγεθος π.χ. 128-bit πριν υπογραφούν (π.χ. hashed RSA)



J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Αλγόριθμοι Δημόσιου Κλειδιού

Ψηφιακή Υπογραφή με τον RSA

CONSTRUCTION 13.10

Let GenRSA be as in the previous sections, and let H be a function with domain $\{0,1\}^*$ and whose range can be set to $\mathbb{Z}_N^*$ for any N. Construct a signature scheme as follows:

- Gen: on input 1^n, run GenRSA(1^n) to compute (N, e, d) and set the range of H to be $\mathbb{Z}_N^*$. The public key is $\langle N, e \rangle$ and the private key is $\langle N, d \rangle$.
- Sign: on input a private key $\langle N, d \rangle$ and a message $m \in \{0,1\}^*$, compute
$$\sigma := [H(m)^d \bmod N].$$
- Vrfy: on input a public key $\langle N, e \rangle$, a message m, and a signature σ, output 1 if and only if $\sigma^e \stackrel{?}{=} H(m) \bmod N$.

The RSA-FDH signature scheme.

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμοι Ψηφιακής Υπογραφής

Ο αλγόριθμος Rabin

Algorithm Key generation for the Rabin public-key signature scheme

1. Generate two large distinct random primes p and q, each roughly the same size.
2. Compute $n = pq$.
3. A's public key is n; A's private key is (p, q).

Algorithm Rabin signature generation and verification

1. *Signature generation.* Entity A should do the following:
   (a) Compute $\tilde{m} = R(m)$.
   (b) Compute a square root s of $\tilde{m} \bmod n$ (using Algorithm 3.44).
   (c) A's signature for m is s.
2. *Verification.* To verify A's signature s and recover the message m, B should:
   (a) Obtain A's authentic public key n.
   (b) Compute $\tilde{m} = s^2 \bmod n$.
   (c) Verify that $\tilde{m} \in \mathcal{M}_R$; if not, reject the signature.
   (d) Recover $m = R^{-1}(\tilde{m})$.

Algorithm 10.3: The ElGamal Signature Scheme

Key Setup

The key setup procedure is the same as that for the ElGamal cryptosystems (see §8.12).

(* thus, user Alice's public-key material is a tuple (g, y, p) where p is a large prime number, $g \in \mathbb{F}_p^*$ is a random multiplicative generator element, and $y_A \equiv g^{x_A} \pmod{p}$ for a secret integer $x_A < p - 1$; Alice's private key is x_A. *)

Signature Generation

To create a signature of message $m \in \mathbb{F}_p^*$, Alice picks a random number $\ell \in_U \mathbb{Z}_{p-1}^*$ (i.e., $\ell < p - 1$ and gcd(l, $p - 1$) = 1) and creates a signature pair (r,s) where

Equation 10.4.2

$$r \leftarrow g^{\ell} \pmod{p},$$

$$s \leftarrow \ell^{-1}(m - x_A r) \pmod{p-1}.$$

Signature Verification

Let Bob be a verifier who knows that the public-key material (g, y_A,p) belongs to Alice. Given a message-signature pair (m,(r, s)), Bob's verification procedure is

$$\text{Verify}_{(g,y_A,p)}(m,(r,s)) = \text{True} \quad \text{if}$$

$$r < p \quad \text{and} \quad y_A{}^r r^s \equiv g^m \pmod{p}.$$

Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

- Αλγόριθμοι Ψηφιακής Υπογραφής
  - *Ο αλγόριθμος DSA*

  - *Το πρότυπο DSS (Digital Signature Standard)*

(US NIST 1991)

Algorithm 10.5: The Digital Signature Standard

Setup of System Parameters

(* the system parameters are identical to those for the Schnorr signature scheme; thus, parameters (*p*, *q*, *g*, *H*), which have the same meaning as those in Alg 10.4, are publicized for use by the system-wide users. *)

Setup of a Principal's Public/Private Key

User Alice picks a random number $x \in_U \mathbb{Z}_q$ as her private key, and computes her public key by

$$y \leftarrow g^x \pmod{p}.$$

Alice's public-key material is (*p*, *q*, *g*, *y*, *H*); her private key is *x*.

Signature Generation

To create a signature of message $m \in \{0, 1\}^*$, Alice picks a random number $\ell \in_U \mathbb{Z}_q$ and computes a signature pair (*r*, *s*) where

$$r \leftarrow (g^\ell \pmod{p}) \pmod{q},$$
$$s \leftarrow \ell^{-1}(H(m) + xr) \pmod{q}.$$

Signature Verification

Let Bob be a verifier who knows that the public-key material (*p*, *q*, *g*, *y*, *h*) belongs to Alice. Given a message-signature pair (*m*, (*r*, *s*)), Bob's verification procedure is

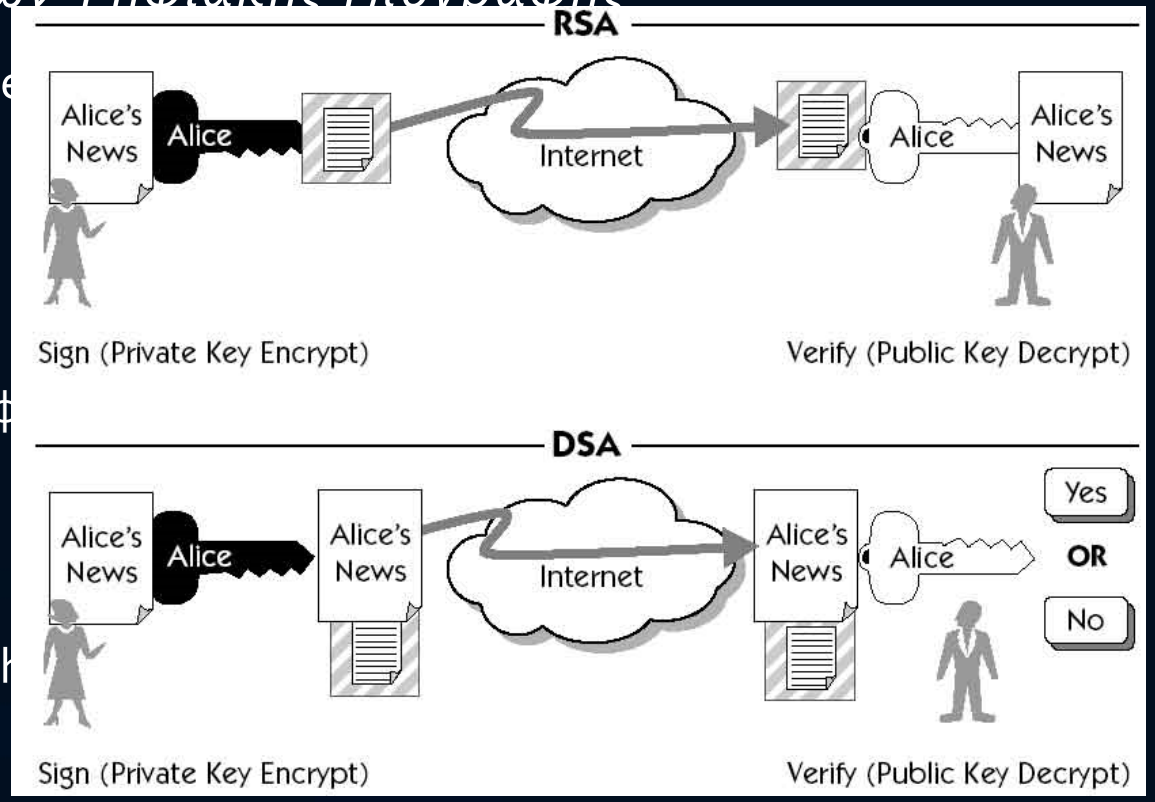
$$w \leftarrow s^{-1} \pmod{q},$$
$$u_1 \leftarrow H(m)w \pmod{q},$$
$$u_2 \leftarrow rw \pmod{q},$$
$$\text{Verify}_{(p,q,g,y,h)}(m, (r, s)) = \text{True} \text{ if } r = (g^{u_1} y^{u_2} \pmod{p}) \pmod{q}.$$

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2000

Συστήματα Δημόσιου Κλειδιού

Διαφοροποιήσεις Συστημάτων Ψηφιακής Υπογραφής

- Ανάκτηση μηνύματος (message recovery)
  - Το μήνυμα ανακτάται κατά την επαλήθευση
  - Δεν είναι απαραίτητο να επισυναφ στην υπογραφή
    - π.χ. RSA, Rabin,...
- Υπογραφή με επισύναψη (with Appendix)
  - Το μήνυμα επισυνάπτεται στην υπογραφή



Στην πράξη, τα μηνύματα «συμπιέζονται» (hash) πριν υπογραφούν! Άρα, το μήνυμα M πρέπει να επισυναφθεί (αφού, οι κρυπτογραφικές συναρτήσεις hash είναι μονόδρομες)

Ψηφιακή Υπογραφή

Ένας «απλός» Μετασχηματισμός

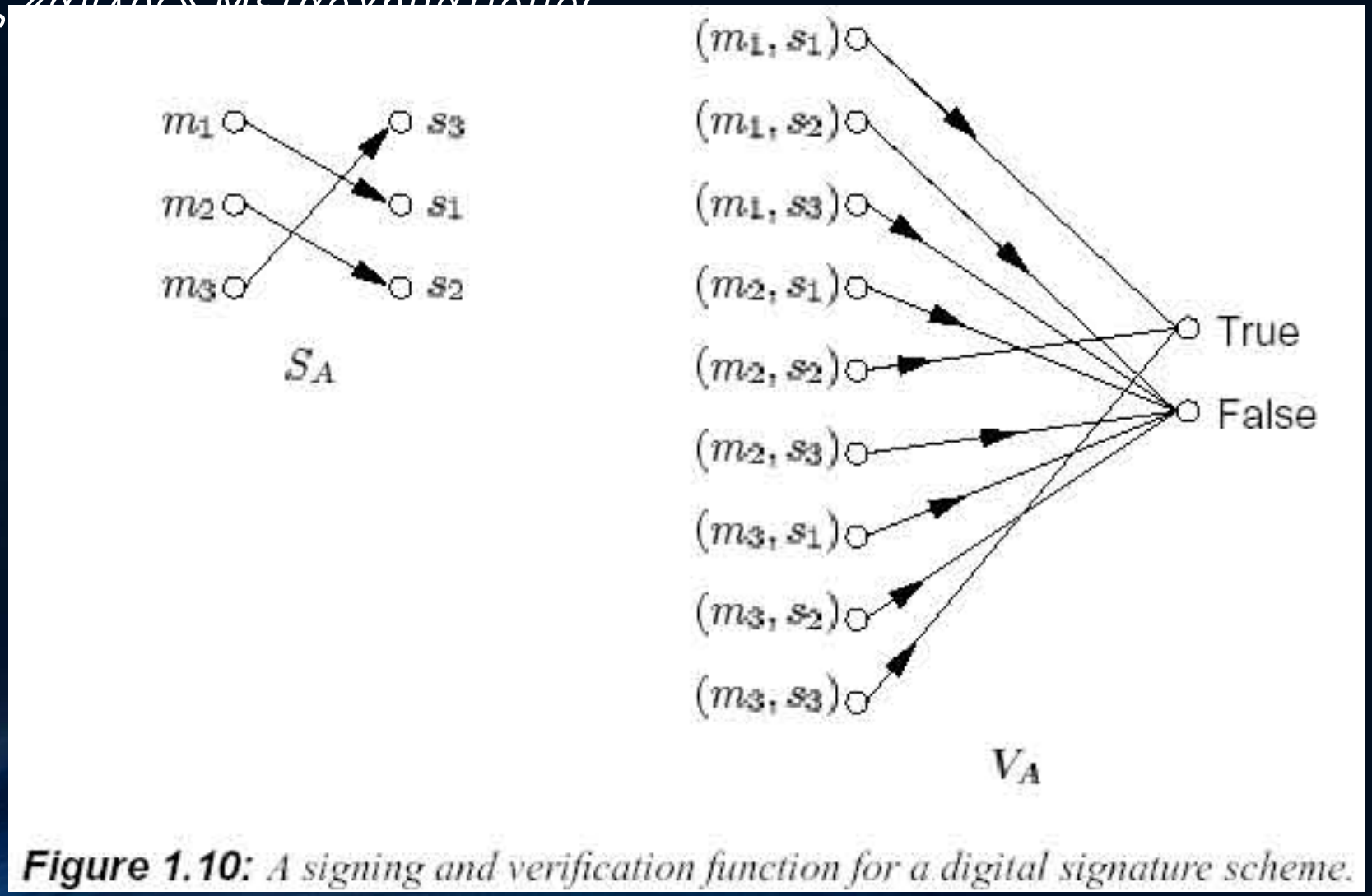


Figure 1.10: *A signing and verification function for a digital signature scheme.*

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Συστήματα Δημόσιου Κλειδιού

Διαφοροποιήσεις Συστημάτων Ψηφιακής Υπογραφής

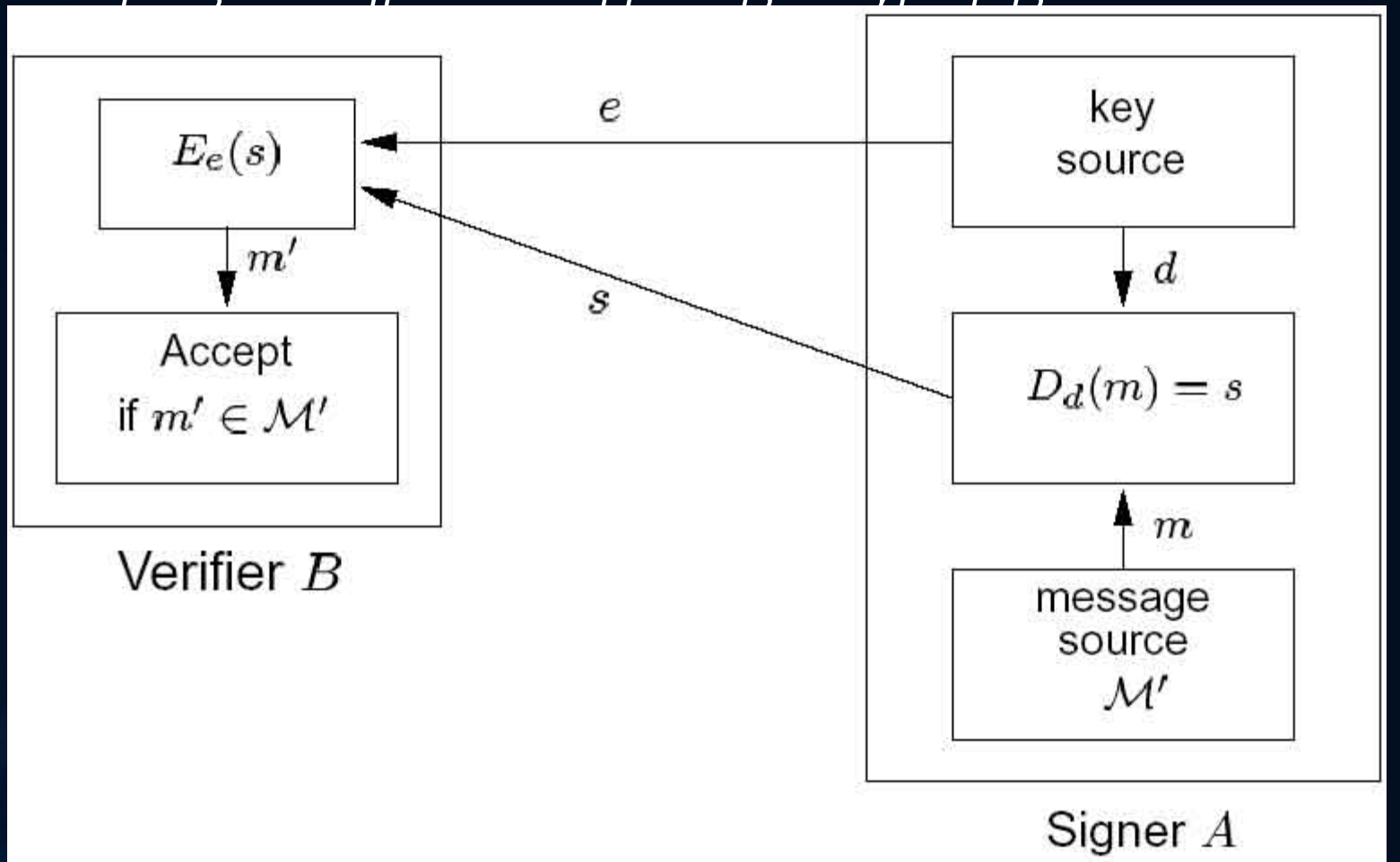


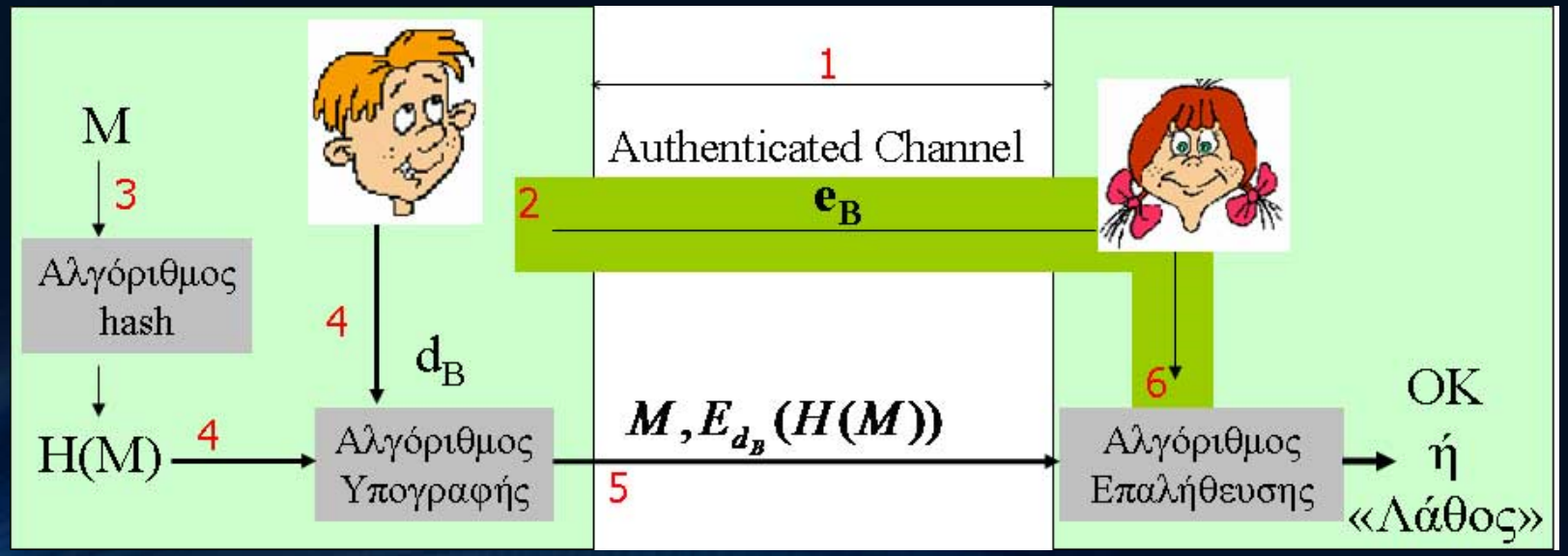
Figure 1.14: *A digital signature scheme with message recovery.* (π.χ. RSA)

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Αλγόριθμοι Δημόσιου Κλειδιού

Ψηφιακή Υπογραφή και Κρυπτογραφικές Συναρτήσεις Hash

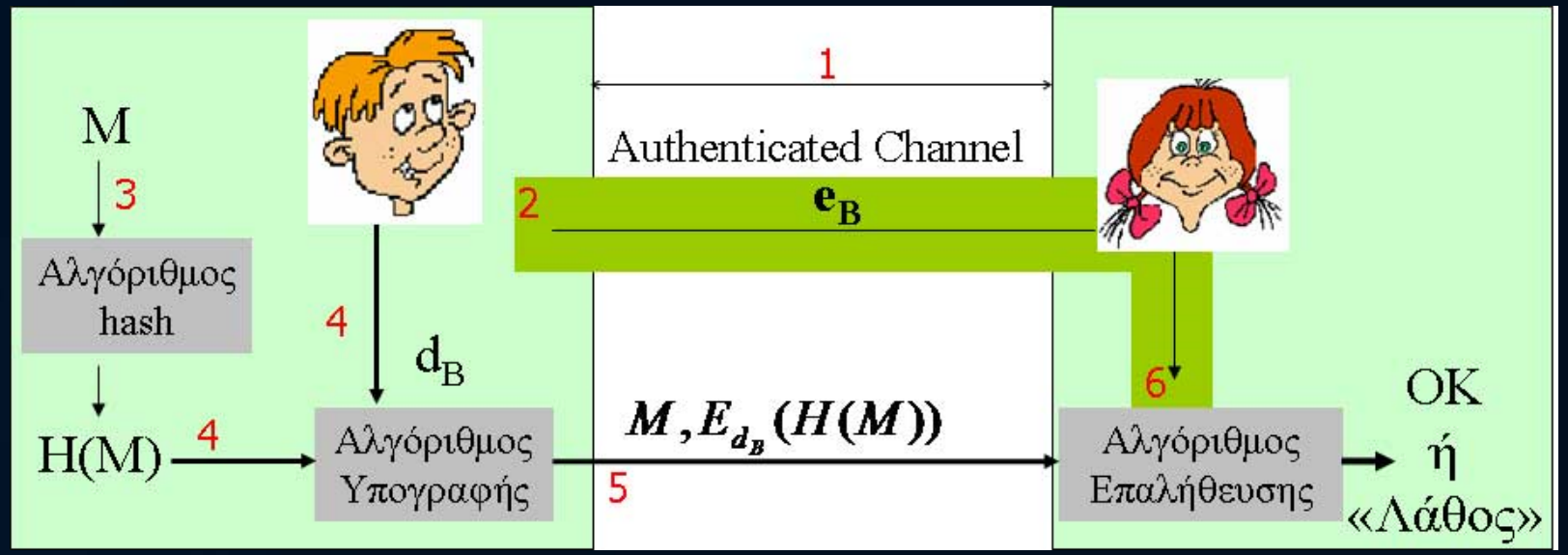
- Ο Bob υπολογίζει την τιμή hash H(M) του μηνύματος M
- Ο Bob υπογράφει το H(M)
- Ο Bob στέλνει το M, καθώς και τη ψηφιακή υπογραφή στην Alice
- Η Alice υπολογίζει την τιμή hash του μηνύματος M, έστω H'(M)
- Η Alice εισάγει το H'(M), την υπογραφή και το ΔΚ του Bob στον αλγόριθμο επαλήθευσης



Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Αλγόριθμοι Δημόσιου Κλειδιού

Ψηφιακή Υπογραφή και Κρυπτογραφικές Συναρτήσεις Hash



- Ο αλγόριθμος προσφέρει αυθεντικότητα-ακεραιότητα
  - Εφόσον η συνάρτηση hash είναι ασφαλής !! (Collision Resistant)
- Τι θα γίνει αν ο Bob επιθυμεί (και) μυστικότητα για το μήνυμα που υπέγραψε;
  - Περίπτωση: Ο Bob υπογράφει το μήνυμα και στη συνέχεια το κρυπτογραφεί

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

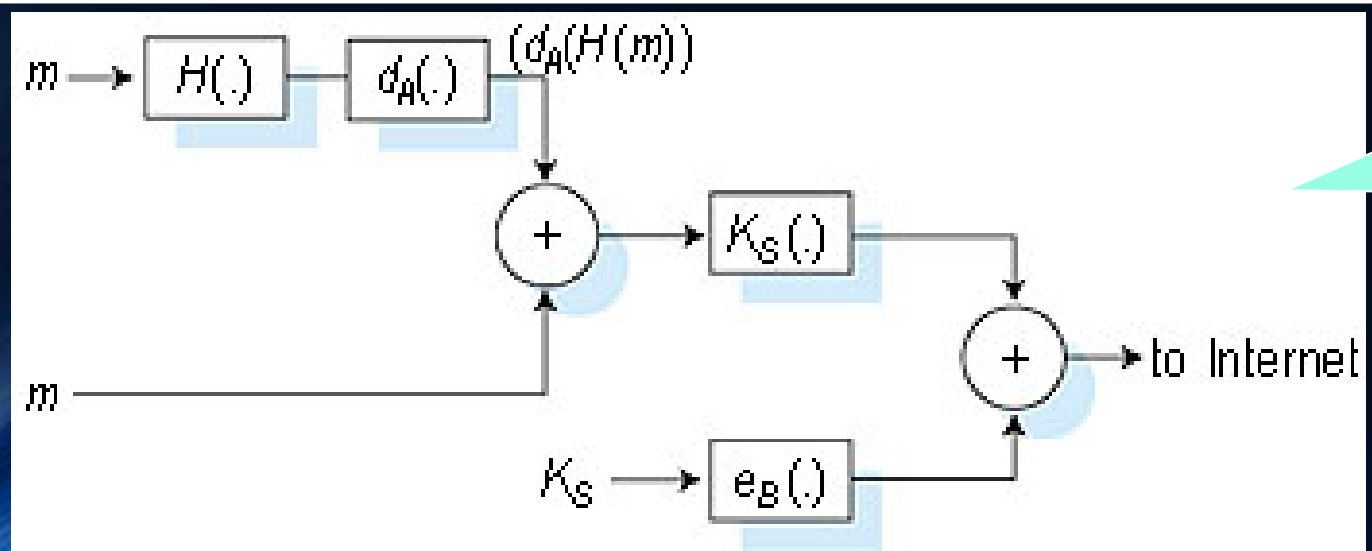
Συνδυασμός Κρυπτογράφησης και Ψηφιακής Υπογραφής

Η Alice

1. Υπογράφει το μήνυμα με το ιδιωτικό της κλειδί IK_A :
2. κρυπτογραφεί την υπογραφή με το ΔK_B του Bob και του το στέλνει

Ο Bob

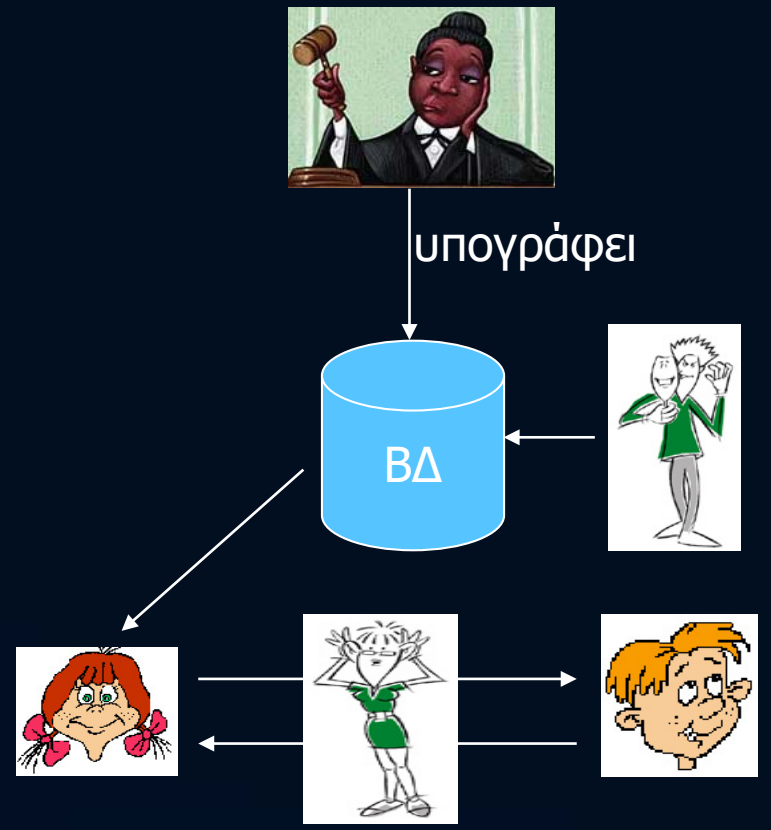
1. Αποκρυπτογραφεί το μήνυμα με το IK_B
2. επαληθεύει την υπογραφή με το ΔK_A της Alice



Παραλλαγή (PGP), χρησιμοποιώντας υβριδικό σύστημα

Συστήματα Δημόσιου Κλειδιού
Ανάγκη για Αυθεντικοποίηση

- Θυμάστε το πρόβλημα της Ενδιάμεσης Οντότητας;
  - Ο Mallory αντικαθιστά το $ΔK_B$ του Bob με το δικό του ($ΔK_M$) στη ΒΔ
- Αν όλα τα ζεύγη (Όνομα, ΔΚ) ήταν ψηφιακά υπογεγραμμένα από μια έμπιστη οντότητα, τότε:
  - Η δουλειά του Mallory θα ήταν δυσκολότερη…



Πιστοποιητικά Δημόσιου Κλειδιού

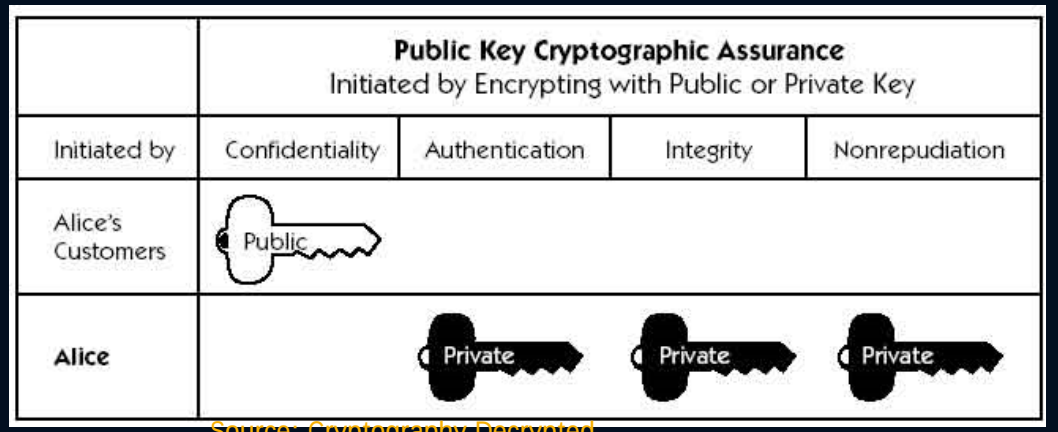
Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Συστήματα Δημόσιου Κλειδιού

Αυθεντικοποίηση και Μη Αποποίηση Ευθύνης

- Η ψηφιακή υπογραφή παρέχει αυθεντικοποίηση μηνύματος
  - Data Origin Authentication

Ερώτηση: Ποια είναι η διαφορά μεταξύ αυθεντικοποίηση μηνύματος και αυθεντικοποίηση χρήστη;



Source: Cryptography Decrypted

  - Αυθ. Μηνύματος: Τώρα ή Κάποτε
  - Αυθ. Χρήστη (Ταυτοποίηση): Τώρα
- Η ψηφιακή υπογραφή μπορεί να προσφέρει μη αποποίηση ευθύνης;
  - Ναι, εφόσον η μυστικότητα του IK του χρήστη προστατεύεται
- Τι θα γίνει εάν ο χρήστης εσκεμμένα αποκαλύψει το IK του;
  - Παρεμφερές πρόβλημα: Συναλλαγές με Κάρτες

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

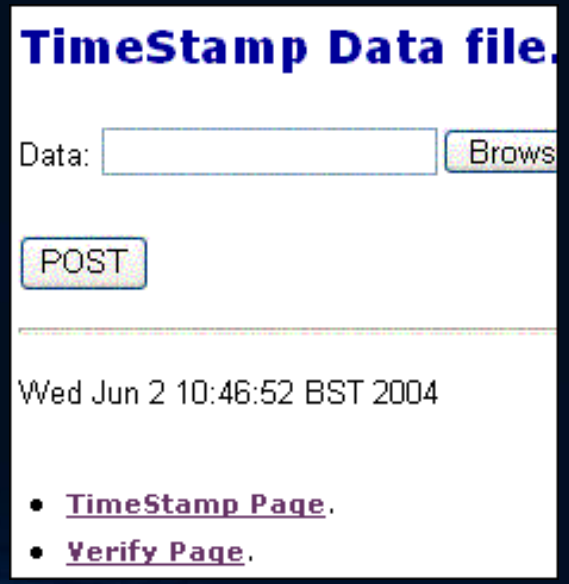
Συστήματα Δημόσιου Κλειδιού

Αυθεντικοποίηση και Μη αποποίηση Ευθύνης

- Πώς αντιμετωπίζεται η απειλή;
  1. Αποτρέπεται η πρόσβαση στο ΙΚ
     - Χρήση έξυπνων καρτών (tamper resistant smart cards
  2. Έμπιστες Υπηρεσίες
     - Ηλ. Υπηρεσίες Χρονοσήμανσης (timestamping services)

Source: www.cardweb.com/

Ο παραλήπτης του υπογεγραμμένου μηνύματος αποτείνεται στην online υπηρεσία που επισυνάπτει μια χρονοσήμανση στο υπογεγραμμένο κείμενο και στη συνέχεια το υπογράφει εκ νέου



Source: http://www.iss.soton.ac.uk

Βιβλιογραφία Διάλεξης

- Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.
- H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2001
- Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001
- N. Ferguson, B. Schneier. Practical Cryptography. Wiley, 2003.
- Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003
- A. Young, M. Yung. Malicious Cryptography – Exploring CryptoVirology. Wiley, 2004
- John Hershey. Cryptography Demystified. McGraw-Hill Professional, 2003
- J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.
- N. Koblitz. A course in Number Theory and Cryptography. 2nd Edition, 1994