ΕΝΝΟΙΕΣ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

Δ. Ζήνδρος

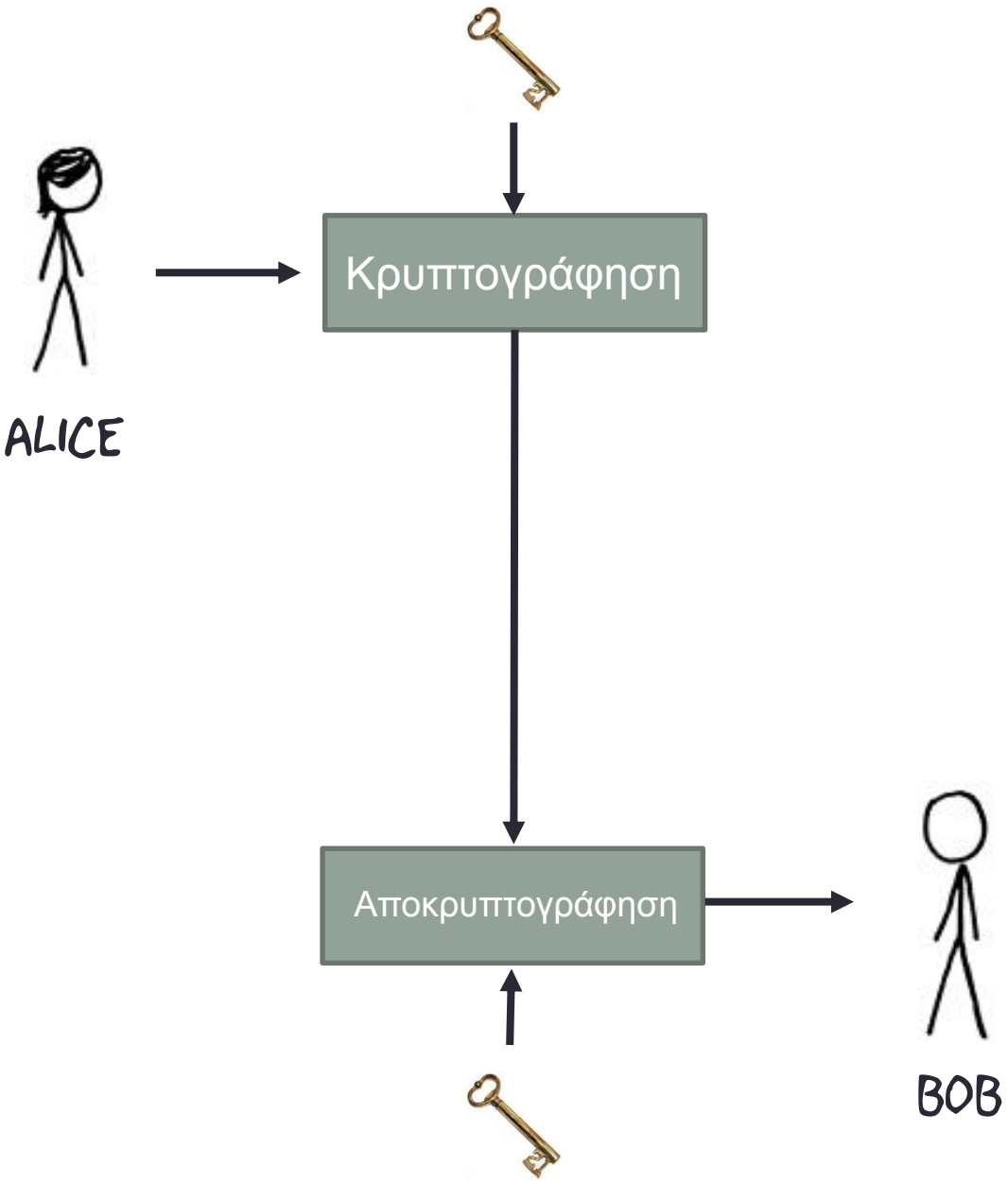
Επιμέλεια διαφανειών: Π. Αγγελάτος, Δ. Ζήνδρος

Στόχος της παρουσίασης

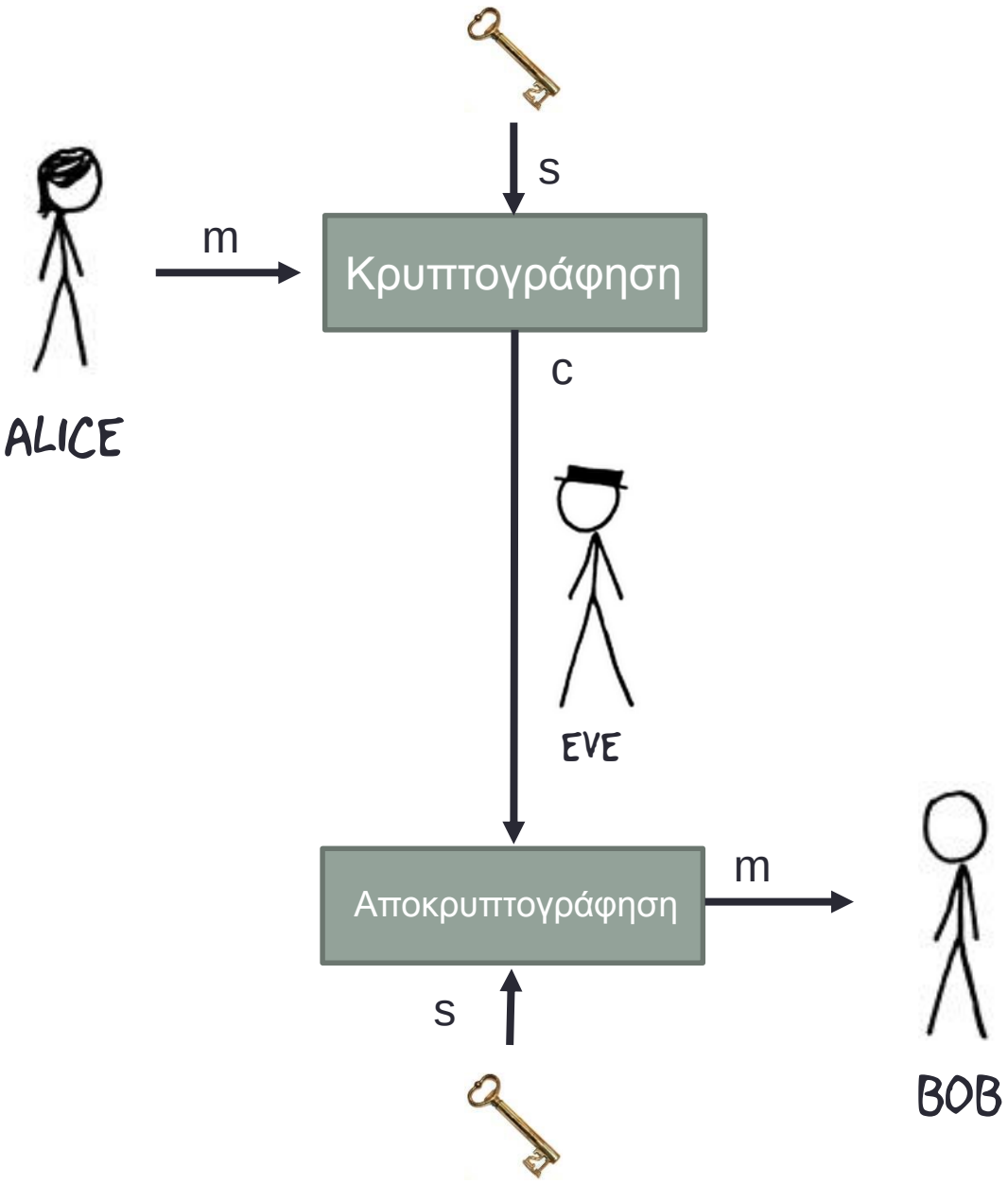
- Έννοιες στην κρυπτογραφία
- Συμμετρική κρυπτογραφία
- AES
- Ασύμμετρη κρυπτογραφία
- RSA
- DSA
- Κρυπτογράφηση & αποκρυπτογράφηση μηνυμάτων
- Ψηφιακές υπογραφές & επιβεβαίωση
- Ανταλλαγή κλειδιών
- Diffie-Hellman

Συμμετρική κρυπτογραφία

- Η Alice θέλει να στείλει ένα μήνυμα στον Bob
- Δεν θέλει να το διαβάσουν άλλοι
- Μοιράζονται ένα **κοινό μυστικό κλειδί**
- Η Alice κρυπογραφεί το μήνυμά της με το κλειδί
- Στέλνει στο δίκτυο το κρυπτογραφημένο κείμενο
- Ο Bob λαμβάνει το κρυπτογραφημένο κείμενο
- Ο Bob αποκρυπτογραφεί το κρυπτογραφημένο κείμενο με το κλειδί
- Λαμβάνει το αρχικό κείμενο


Κρυπτογράφηση
ALICE
Αποκρυπτογράφηση
BOB

- m
  - message – καθαρό κείμενο
- s
  - secret – μυστικό κλειδί
- c = E(s, m)
  - encrypt – κρυπτογράφηση m με κλειδί s
  - δίνει ως αποτέλεσμα κρυπτοκείμενο c
- m = D(s, c)
  - decrypt – αποκρυπτογράφηση c με κλειδί s
  - δίνει ως αποτέλεσμα το καθαρό κείμενο m
- Ορθότητα: D(s, E(s, m)) = m


s
m
Κρυπτογράφηση
ALICE
c
EVE
Αποκρυπτογράφηση
m
s
BOB

Threat models

- Δε μιλάμε γενικά για «ασφαλή» ή «ανασφαλή» συστήματα
- Ορίζουμε τι είδους ασφάλεια θέλουμε
- Δε γίνεται ένα σύστημα να είναι απόλυτα «ασφαλές»
- Ποιος είναι ο εχθρός μας;
  - Ένας φίλος που μας κάνει πλάκα;
  - Ένας πρώην σύζυγος;
  - Ένας εταιρικός κατάσκοπος;
  - Μία κυβέρνηση;
  - Οι μυστικές υπηρεσίες;
- Πόσα χρήματα μπορεί να ξοδέψει ο εχθρός μας;
- Πόσο χρόνο μπορεί να ξοδέψει ο εχθρός μας;

Threat models

- Αναρωτηθείτε
- Για να «χακάρει» κάποιος ένα website
  - Είναι πιο φθηνό να «σπάσει» ένα κρυπτογραφικό κλειδί;
  - ...ή να «λαδώσει» ένα προγραμματιστή;
- Για να κλέψει κάποιοες δεδομένα από τον υπολογιστή σου
  - Είναι πιο φθηνό να φτιάξει και να σε μολύνει με έναν ιό;
  - ...ή να τον χρησιμοποιήσει όταν τον ξεχάσεις ξεκλείδωτο;
- Για να διαβάσει κάποιος τα κρυπτογραφημένα μηνύματά σου
  - Είναι πιο εύκολο να παραβιάσει την κρυπτογραφία;
  - ...ή να αλλάξει το πληκτρολόγιό σου σε ένα κατασκοπικό;

Συμμετρική κρυπτογραφία

- Σήμερα χρησιμοποιούμε το σύστημα AES
- Γρήγορη
- Για κρυπτογράφηση σε σκληρούς δίσκους
- Για κρυπτογράφηση πολλών δεδομένων στο δίκτυο

Προβλήματα συμμετρικής κρυπτογραφίας

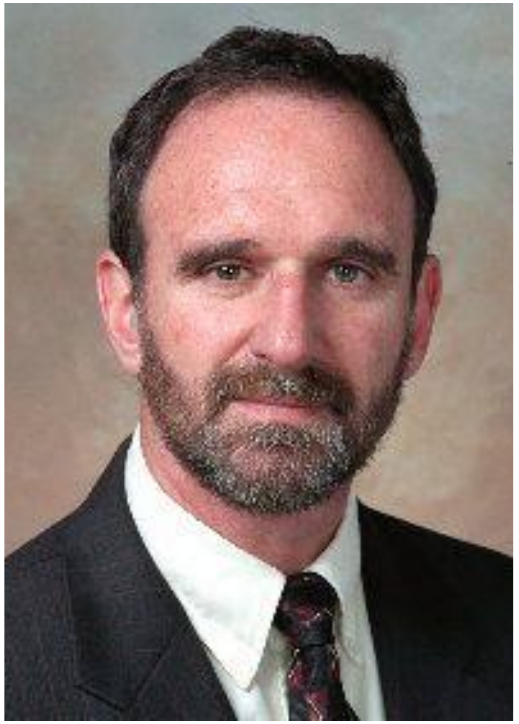
- Κάθε ζεύγος ανθρώπων χρειάζεται ένα κλειδί
- n άνθρωποι → ~n^2 κλειδιά
- Τα κλειδιά πρέπει να μείνουν μυστικά
- Κάπως πρέπει να τα ανταλλάξουν

Ασύμμετρη κρυπτογραφία

- Diffie & Hellman, 1976
- RSA – Rivest, Shamir, Adleman, 1977
- Νέα ιδέα:
  - Κάθε άνθρωπος έχει ένα **ζεύγος κλειδιών**:
  - Ιδιωτικό κλειδί & Δημόσιο κλειδί
  - Τα κλειδιά συνδέονται μαθηματικά
  - Για κάθε ιδιωτικό κλειδί υπάρχει μοναδικό δημόσιο
  - Για κάθε δημόσιο κλειδί υπάρχει μοναδικό ιδιωτικό
  - Από το ιδιωτικό μπορούμε να βρούμε το δημόσιο
  - Από το δημόσιο δεν μπορούμε να βρούμε το ιδιωτικό

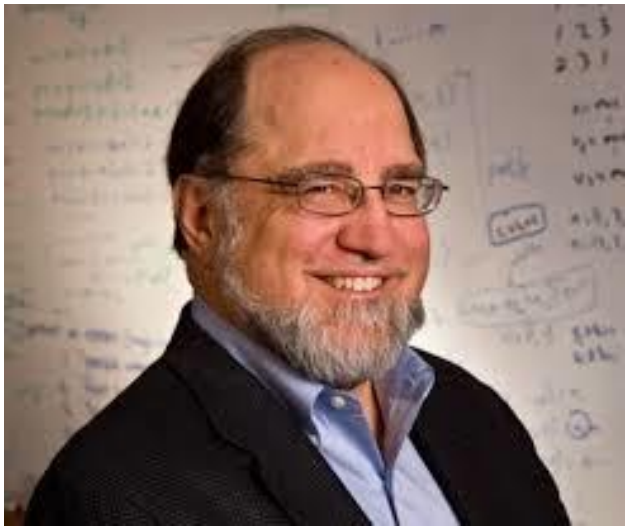
Diffie & Hellman

Whitfield Diffie

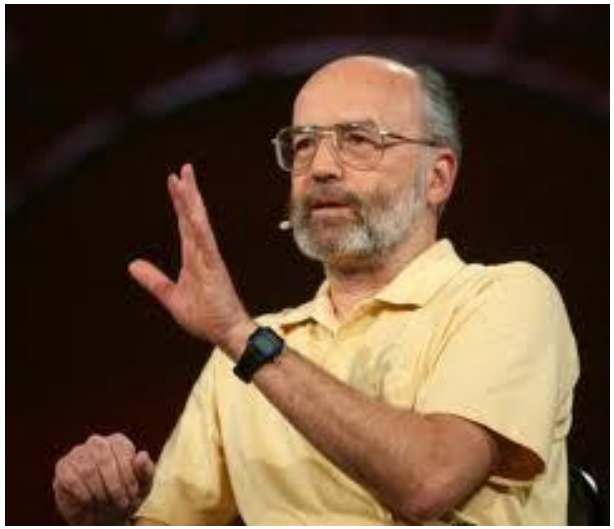


Martin Hellman

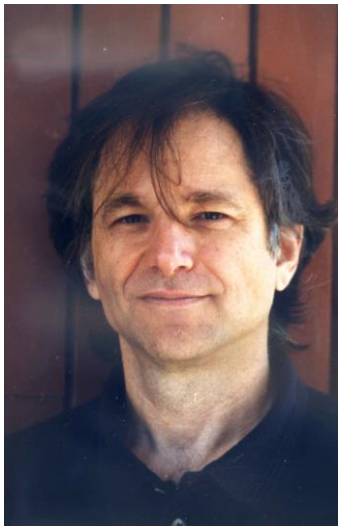
RSA



Ron Rivest



Adi Shamir



Leonard Adleman

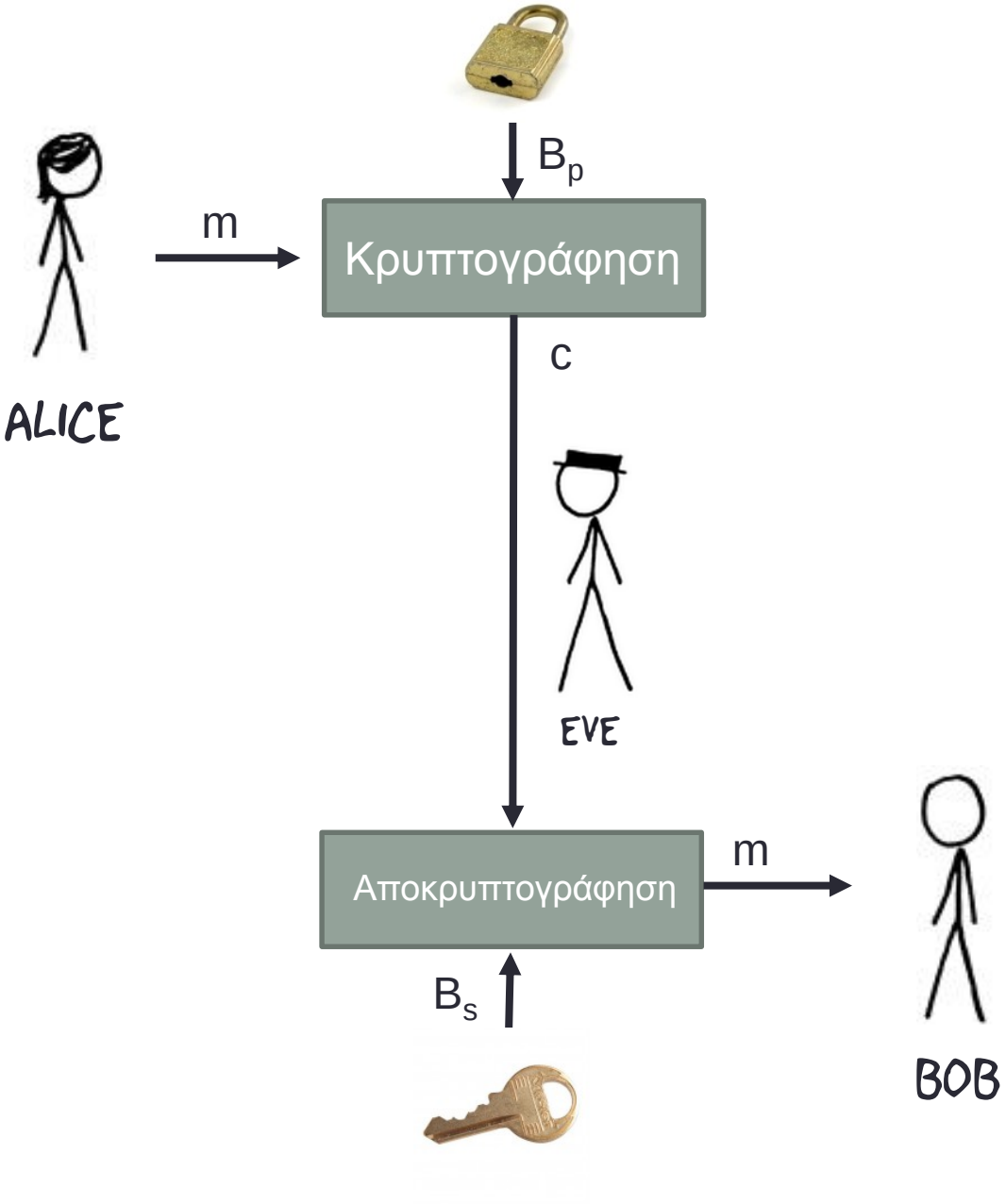
Ασύμμετρη κρυπτογραφία

- Αρχή λειτουργίας:
  - Ό,τι κρυπτογραφείται με το δημόσιο κλειδί κάποιου, αποκρυπτογραφείται από το αντίστοιχο ιδιωτικό του.
  - Ό,τι κρυπτογραφείται με το ιδιωτικό κλειδί κάποιου, αποκρυπτογραφείται από το αντίστοιχο δημόσιο του.

Ασύμμετρη κρυπτογραφία

- Η Alice θέλει να στείλει ένα μήνυμα στον Bob
- Δεν θέλει να το διαβάσουν άλλοι
- Ο καθένας έχει το ιδιωτικό και δημόσιο κλειδί του
- Η Alice κρυπογραφεί το μήνυμά της **με το δημόσιο κλειδί του Bob**
- Στέλνει στο δίκτυο το κρυπτογραφημένο κείμενο
- Ο Bob λαμβάνει το κρυπτογραφημένο κείμενο
- Ο Bob αποκρυπτογραφεί το κρυπτογραφημένο κείμενο **με το ιδιωτικό κλειδί του**
- Λαμβάνει το αρχικό κείμενο

- A_s
  - Alice’s secret – μυστικό κλειδί
- A_p
  - Alice’s public – δημόσιο κλειδί
- B_s
  - Bob’s secret – μυστικό κλειδί
- B_p
  - Bob’s public – δημόσιο κλειδί
- $c = E(B_p, m)$
  - encrypt – κρυπτογράφηση m με κλειδί B_p
  - δίνει ως αποτέλεσμα κρυπτοκείμενο c
- $m = D(B_s, c)$
  - decrypt – αποκρυπτογράφηση c με κλειδί B_s
  - δίνει ως αποτέλεσμα το καθαρό κείμενο m
- Ορθότητα: $D(B_s, E(B_p, m)) = m$


B_p
m
Κρυπτογράφηση
c
ALICE
EVE
Αποκρυπτογράφηση
m
B_s
BOB

Συμμετρική κρυπτογραφία

- Γρήγορη απόδοση
- Μοιρασμένο μυστικό
- n^2 κλειδιά
- Δυσκολία ανταλλαγής κλειδιών

Ασύμμετρη κρυπτογραφία

- Αργή απόδοση
- Ο καθένας έχει το δικό του ζεύγος κλειδιών
- n κλειδιά
- Δεν υπάρχει ανάγκη ανταλλαγής κλειδιών

Από την θεωρία στην πράξη

- PGP
  - Pretty Good Privacy
  - Όρισε το OpenPGP πρωτόκολλο για κρυπτογράφηση/αποκρυπτογράφηση
  - Πρώτη ευρείας χρήσης ασύμμετρη κρυπτογραφία
  - Phil Zimmermann, 1991
- GPG
  - Ελεύθερη υλοποίηση

Phil Zimmermann

Quiz

- Η Alice στέλνει ένα κρυπτογραφημένο μήνυμα στον Bob
- Πριν το στείλει θέλει να επιβεβαιώσει ότι είναι σωστό
- Μπορεί να αποκρυπτογραφήσει αυτό που κρυπτογράφησε;

Quiz

- Η Alice στέλνει ένα κρυπτογραφημένο μήνυμα στον Bob
- Πριν το στείλει θέλει να επιβεβαιώσει ότι είναι σωστό
- Μπορεί να αποκρυπτογραφήσει αυτό που κρυπτογράφησε;
- Όχι!
- Η κρυπτογράφηση έγινε με το δημόσιο κλειδί του Bob.
- Η Alice δεν έχει το ιδιωτικό κλειδί του Bob.
- Ό,τι κρυπτογραφείται με το δημόσιο κλειδί κάποιου, αποκρυπτογραφείται με το αντίστοιχο ιδιωτικό!

Ασύμμετρη κρυπτογραφία

- Άρχή λειτουργίας:
  - Ό,τι κρυπτογραφείται με το δημόσιο κλειδί κάποιου, αποκρυπτογραφείται από το αντίστοιχο ιδιωτικό του.
  - **Ό,τι κρυπτογραφείται με το ιδιωτικό κλειδί κάποιου, αποκρυπτογραφείται από το αντίστοιχο δημόσιο του.**

- **Γιατί χρειάζεται αυτό;**

Quiz

- Τι συμβαίνει αν η Alice κρυπτογραφήσει ένα μήνυμα με το ιδιωτικό κλειδί της;
- Ποιος μπορεί να το διαβάσει;

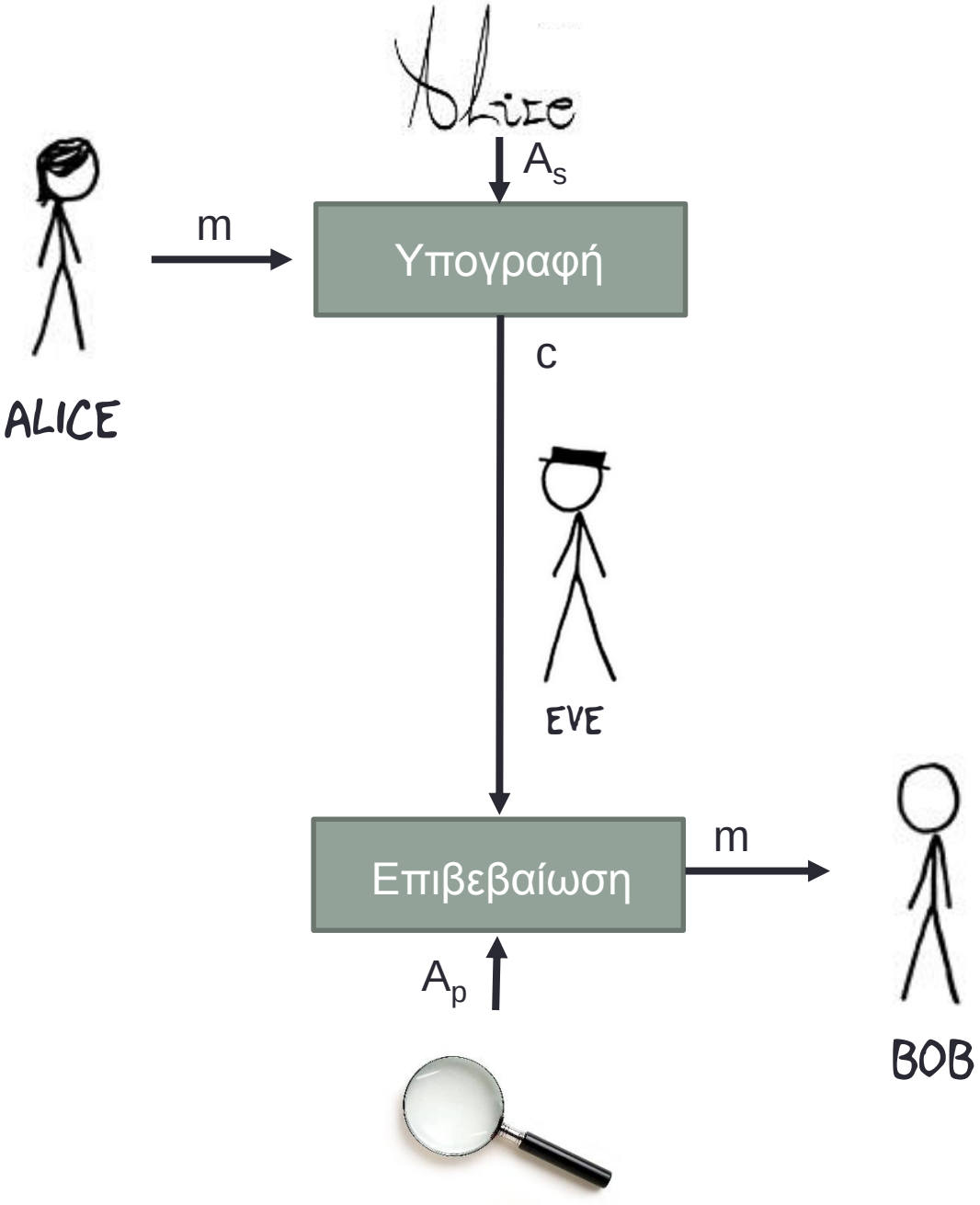
Ψηφιακές υπογραφές

- Η Alice θέλει να στείλει ένα μήνυμα στον Bob
- Ο Bob θέλει να επιβεβαιώσει ότι το έγραψε η Alice
- Ο καθένας έχει το ιδιωτικό και δημόσιο κλειδί του
- Η Alice κρυπογραφεί το μήνυμά της με το **ιδιωτικό κλειδί της**
- Στέλνει στο δίκτυο το κρυπτογραφημένο κείμενο
- Ο Bob λαμβάνει το κρυπτογραφημένο κείμενο
- Ο Bob αποκρυπτογραφεί το κρυπτογραφημένο κείμενο με το **δημόσιο κλειδί της Alice**
- Λαμβάνει το αρχικό κείμενο

Ψηφιακές υπογραφές

- Η Alice θέλει να στείλει ένα μήνυμα στον Bob
- Ο Bob θέλει να επιβεβαιώσει ότι το έγραψε η Alice
- Ο καθένας έχει το ιδιωτικό και δημόσιο κλειδί του
- Η Alice **υπογράφει** το μήνυμά της με το **ιδιωτικό κλειδί της**
- Στέλνει στο δίκτυο το **υπογεγραμμένο** κείμενο
- Ο Bob λαμβάνει το **υπογεγραμμένο** κείμενο
- Ο Bob **επιβεβαιώνει** το υπογεγραμμένο κείμενο με το **δημόσιο κλειδί της Alice**

- A_s
  - Alice's secret – μυστικό κλειδί
- A_p
  - Alice's public – δημόσιο κλειδί
- B_s
  - Bob's secret – μυστικό κλειδί
- B_p
  - Bob's public – δημόσιο κλειδί
- $c = S(B_s, m)$
  - sign – υπογραφή του μηνύματος m με κλειδί B_s
  - δίνει ως αποτέλεσμα κρυπτοκείμενο c
- $m = V(B_p, c, m)$
  - verify – επιβεβαίωση υπογραφής c με κλειδί B_p
- Ορθότητα: $V(B_p, S(B_p, m), m) = true$


Alice
A_s
m
Υπογραφή
c
ALICE
EVE
Επιβεβαίωση
m
A_p
BOB

Ψηφιακές υπογραφές

- Πιο ασφαλείς από τις συμβατικές υπογραφές
- Δεν μπορούν να παραχαρακτούν
- Περιλαμβάνουν το αρχικό καθαρό κείμενο μαζί με την υπογραφή
- Είναι **συνδεδεμένες** με το κείμενο που υπογράφονται
- Κάθε υπογραφή είναι διαφορετική και εξαρτάται από το κείμενο
- Αν αλλάξει το κείμενο, η υπογραφή δεν είναι πια έγκυρη!
- Δεν γίνεται να αντιγράψω μία υπογραφή και να τη βάλω σε άλλο κείμενο
- Είστε ενδεχομένως νομικά υπεύθυνοι γι’ αυτές!

Μαθηματικά κρυπτογραφίας

- Η κρυπτογραφία στηρίζεται σε one-way προβλήματα
- Πολυωνυμικά υπολογίζονται προς τη μία κατεύθυνση
- Εκθετικά προς την αντίστροφη

Διακριτός λογάριθμος

- $y = b^e \bmod p$
- Δεδομένων b, e, p, η εύρεση του y είναι εύκολη
- Δεδομένων y, b, p, η εύρεση του e είναι δύσκολη

- π.χ. y = 3435, b = 7, p = 7919, e = ?

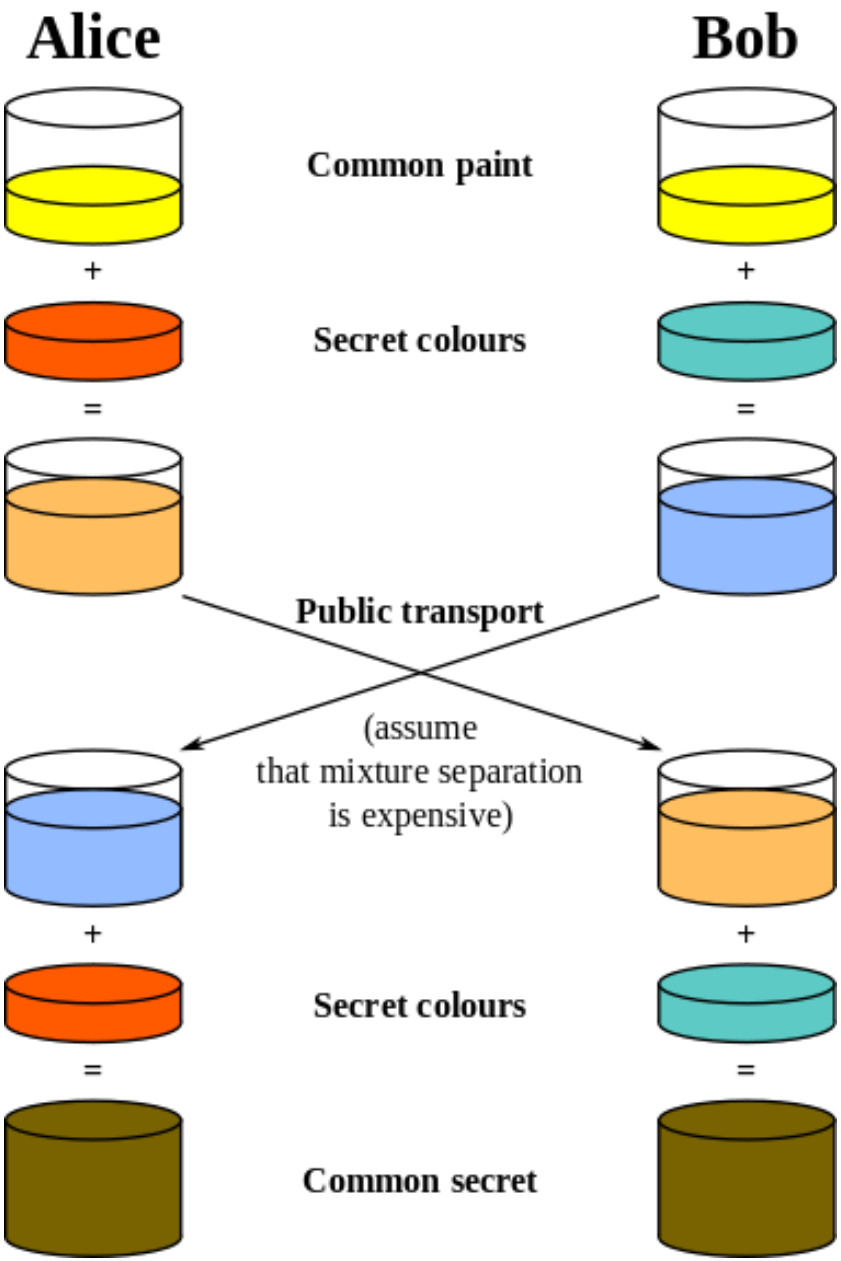
Παραγοντοποίηση

- Έστω p, q πρώτοι και n = pq
- Δεδομένων p, q, η εύρεση του n είναι εύκολη
- Δεδομένου n, η εύρεση των p, q είναι δύσκολη

- π.χ. n = 1263237248027, p = ?, q = ?

Ανταλλαγή κλειδιού

- Alice και Bob θέλουν να συμφωνήσουν σε ένα κοινό κλειδί
- Το κλειδί αυτό θα χρησιμοποιηθεί για συμμετρική κρυπτογραφία
- Έχουν μόνο ένα **δημόσιο** κανάλι επικοινωνίας
- Δεν έχουν προσυμφωνημένα μυστικά


Alice
Bob
Common paint
+
+
Secret colours
=
=
Public transport
(assume
that mixture separation
is expensive)
+
+
Secret colours
=
=
Common secret

Diffie-Hellman

- Alice, Bob: Συμφωνούν σε κοινά p, g, δημόσια
- Alice: Σκέφτεται ένα μυστικό α
- Bob: Σκέφτεται ένα μυστικό β
- Alice: Υπολογίζει και δημοσιεύει $A = g^{\alpha} \pmod p$
- Bob: Υπολογίζει και δημοσιεύει $B = g^{\beta} \pmod p$
- Alice: Υπολογίζει $B^{\alpha} \pmod p = (g^{\beta})^{\alpha} \pmod p = g^{\beta\alpha} \pmod p$
- Bob: Υπολογίζει $A^{\beta} \pmod p = (g^{\alpha})^{\beta} \pmod p = g^{\alpha\beta} \pmod p$
- Αντιμεταθετική ιδιότητα: $g^{\alpha\beta} \pmod p = g^{\beta\alpha} \pmod p = s$
- s μυστικό κλειδί
- Eve: Δεν μπορεί να ανακτήσει το α από το A ή β από το B λόγω διακριτού λογαρίθμου

RSA

- p, q πρώτοι
- n = pq
- e τυχαίος αριθμός από 2 έως n - 2
- d επιλέγεται έτσι ώστε $de = 1 \pmod{\varphi(n)}$
- Κρυπτογράφηση: $c = m^e \pmod{n}$
- Αποκρυπτογράφηση: $m = c^d \pmod{n}$
- Ορθότητα: $m^{ed} = m \pmod{n}$
- Μικρό θεώρημα Fermat: $m^{\varphi(n)} = 1 \pmod{n}$

Μάθαμε

- Έννοιες στην κρυπτογραφία
- Συμμετρική κρυπτογραφία - AES
- Έννοιες στην ασύμμετρη κρυπτογραφία
- RSA
- Κρυπτογράφηση & αποκρυπτογράφηση μηνυμάτων
- Ψηφιακές υπογραφές & επιβεβαίωση
- Ανταλλαγή κλειδιών
- Diffie-Hellman

Ευχαριστώ! Ερωτήσεις;

@dionyziz