ΑΡΗΣ ΠΑΓΟΥΡΤΖΗΣ

–

ΣΤΑΘΗΣ ΖΑΧΟΣ

ΣΧΟΛΗ ΗΜΜΥ

ΕΜΠ

ΥΠΟΛΟΓΙΣΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Εισαγωγή

ΔΙΟΙΚΗΤΙΚΑ ΤΟΥ ΜΑΘΗΜΑΤΟΣ (2022-2023)

- Διδάσκοντες
  - Στάθης Ζάχος
  - Άρης Παγουρτζής
  - Πέτρος Ποτίκας
  - Παναγιώτης Γροντάς
- Βοηθοί διδασκαλίας
  - Pourandokht Behrouz
  - Γιάννης Βρεττός
  - Ορέστης Κωνσταντινίδης
  - Ελένη Μακρή
  - Δανάη Μπάλλα
  - Θωμάς Σουλιώτης
  - Μαριάννα Σπυράκου

ΔΙΟΙΚΗΤΙΚΑ ΤΟΥ ΜΑΘΗΜΑΤΟΣ (2022-2023)

- Ημέρες-ώρες
  - Τρίτη **12:45 – 15:30**
  - Παρασκευή **18:00-19:30**
- Ιστοσελίδα:
  - http://courses.corelab.ntua.gr/crypto
- Βαθμολογικό σχήμα:
  - Ασκήσεις (θεωρητικές / πρακτικές): **3** μονάδες
  - Εργασία (project): **2** μονάδες
  - Τελικό διαγώνισμα: **6** μονάδες (απαραίτητες **2.5**)

ΤΙ ΕΙΝΑΙ Η ΚΡΥΠΤΟΓΡΑΦΙΑ

- Πιο σωστά: Κρυπτολογία
- Η τέχνη της «μεταμφίεσης» της πληροφορίας (*κρυπτογράφηση*)
- …αλλά και της επαναφοράς της στην αρχική μορφή (*αποκρυπτογράφηση*)
- …ακόμη και χωρίς το νόμιμο κλειδί (*κρυπτανάλυση*)
- … και όχι μόνο: ψηφιακές υπογραφές, ταυτοποίηση, ψηφοφορίες, ασφαλείς υπολογισμοί, ψηφιακό χρήμα

ΣΗΜΑΣΙΑ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

- Ασφάλεια επικοινωνιών (πολιτικών και στρατιωτικών)
- Ασφάλεια / διευκόλυνση συναλλαγών
- Κρυπτονομίσματα
- Νομικές εφαρμογές (ψηφιακά συμβόλαια)
- Ανωνυμία, προστασία δεδομένων
- Κοινωνικο-πολιτικός αντίκτυπος (ελευθερία λόγου / τύπου, WikiLeaks, ψηφοφορίες, κοινωνικά δίκτυα)

Η ΟΜΟΡΦΙΑ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

- Υλοποίηση πολλών φαινομενικά αδύνατων λειτουργιών (δημόσιο κλειδί, μηδενική γνώση, πιστοποιημένη ανωνυμία, …)
- Ανάπτυξη πλήθους υπολογιστικών τεχνικών και μεθόδων
- Μαθηματικές αποδείξεις: η θεωρία αριθμών στο επίκεντρο των τεχνολογικών εξελίξεων!

G. H. Hardy, *A mathematician's apology*

ΠΡΟΘΕΡΜΑΝΣΗ: ΕΝΑ ΠΡΟΒΛΗΜΑ

Ποιο ψηφίο λείπει από τον αριθμό 2^{29} ;

(αποτελείται από 9 διαφορετικά ψηφία)

ΤΟ ΠΡΟΒΛΗΜΑ ΤΟΥ 2^{29}

Πόσες πράξεις χρειαζόμαστε;

Γίνεται καλύτερα;

ΤΟ ΠΡΌΒΛΗΜΑ ΤΟΥ 2^{29}

Γίνεται χωρίς να υπολογίσουμε πλήρως τον αριθμό;

(ερώτηση από βιβλίο προετοιμασίας για συνεντεύξεις σε 'quant jobs')

ΣΥΣΤΑΣΕΙΣ

Alice

Bob

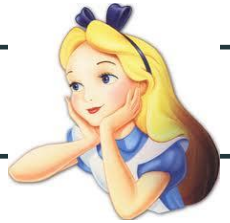
Eve

Mallory

Peggy

Victor

Trent

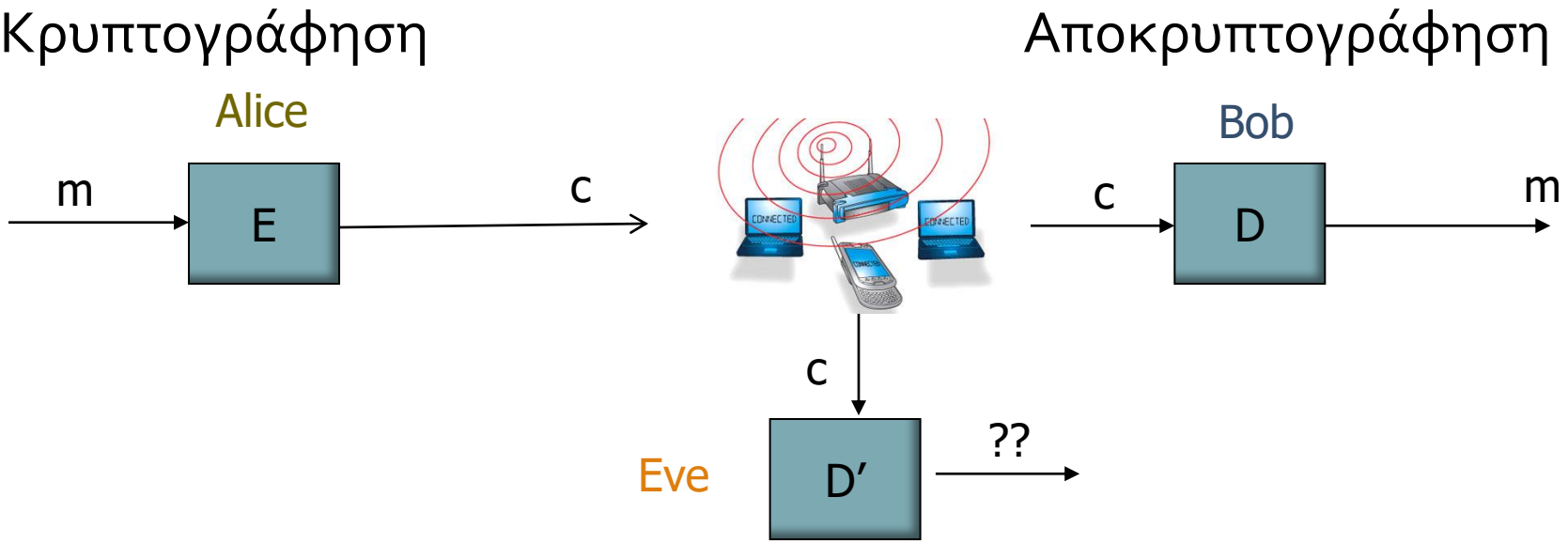


ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

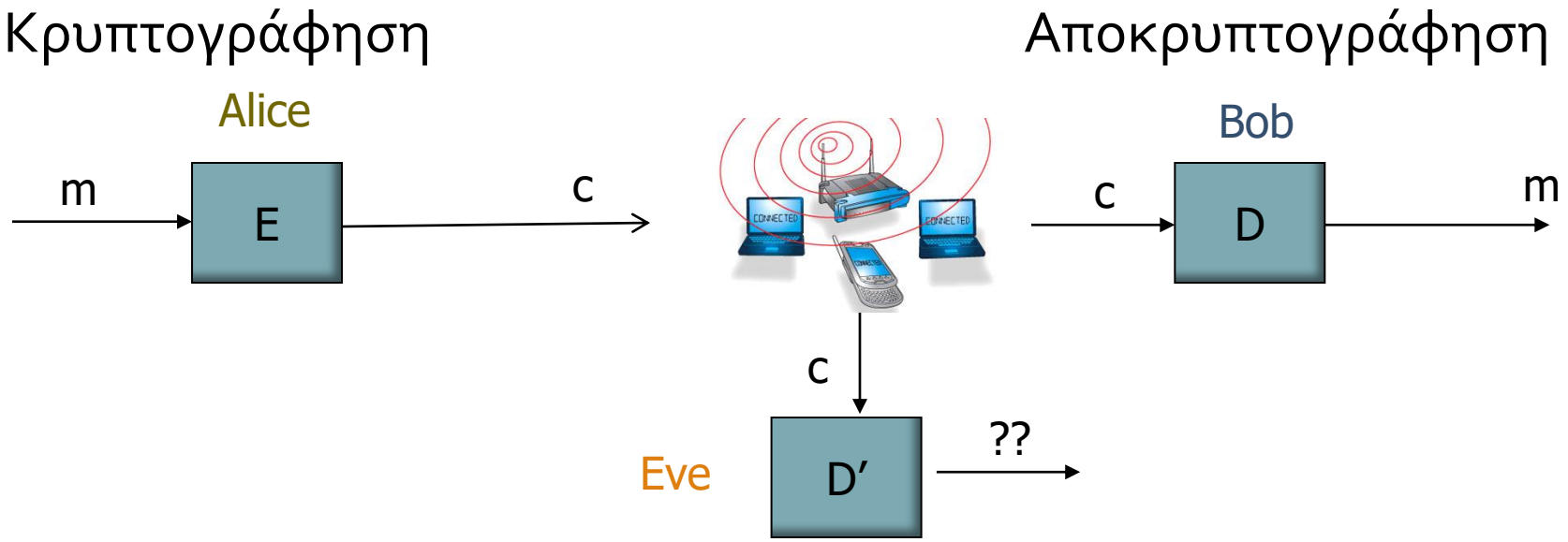
Κρυπτογράφηση

Αποκρυπτογράφηση

ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

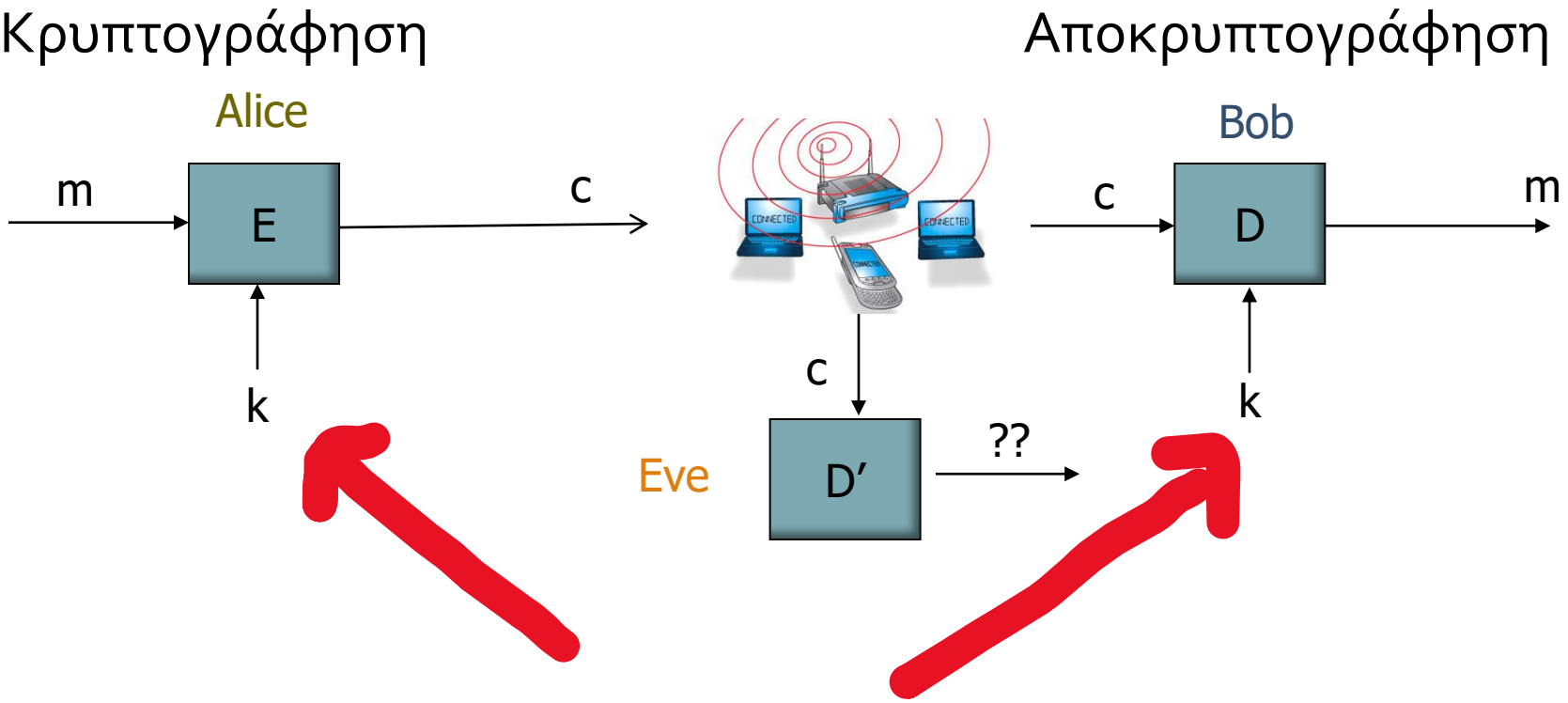


ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ



- … με χρήση *κοινού* ιδιωτικού κλειδιού (συμμετρική κρυπτογραφία)

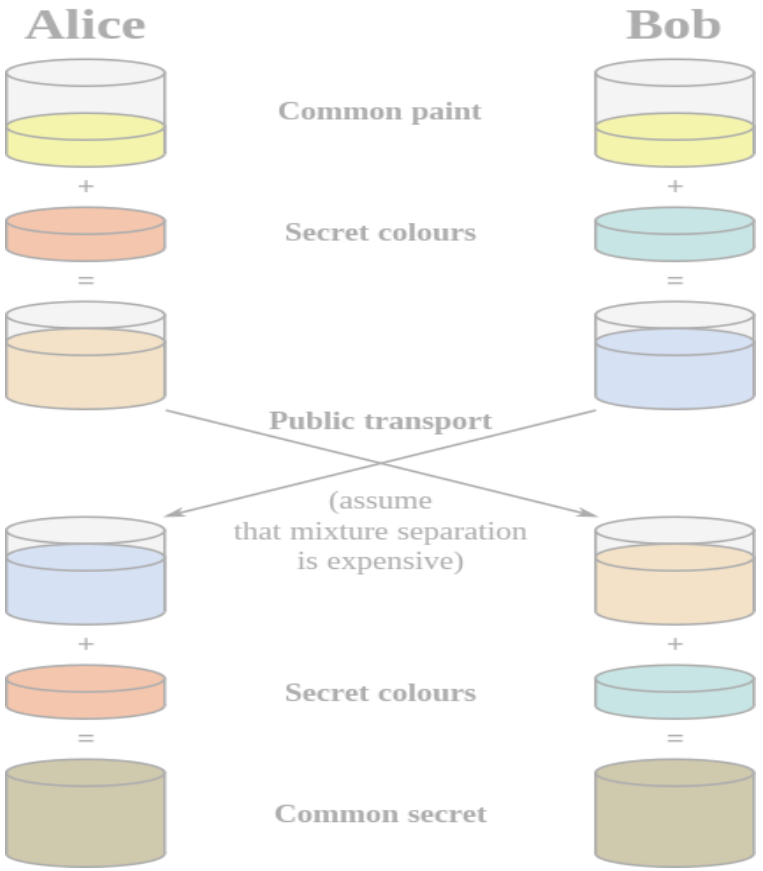
ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ



- … με χρήση *κοινού* ιδιωτικού κλειδιού (συμμετρική κρυπτογραφία)
- Πρόβλημα: *ανταλλαγή κλειδιού?*

ΛΥΣΗ: DIFFIE-HELLMAN KEY EXCHANGE

- Επιλέγονται: πρώτος p, και γεννήτορας g της $\mathbb{Z}_p^* = \{1, ., p-1\}$, γνωστοποιούνται σε A και B.
- B → A: $b^* = g^b \bmod p$
  (b: ιδιωτικό κλειδί του B)
- A → B: $a^* = g^a \bmod p$
  (a: ιδιωτικό κλειδί της A)
- A: $K = (b^*)^a \bmod p = g^{ba} \bmod p$
- B: $K = (a^*)^b \bmod p = g^{ab} \bmod p$
- **Εικασία Diffie-Hellman:** *υπολογιστικά απρόσιτο να υπολογιστεί K από a^*, b^**



A.J. Han Vinck, Introduction to public key cryptography

Διακριτος Λογαριθμος

Δίνονται: πρώτος p, γεννήτορας g της ομάδας $\mathbb{Z}_p^* = \{1, \dots, p-1\}$ και $a \in \mathbb{Z}_p^*$.

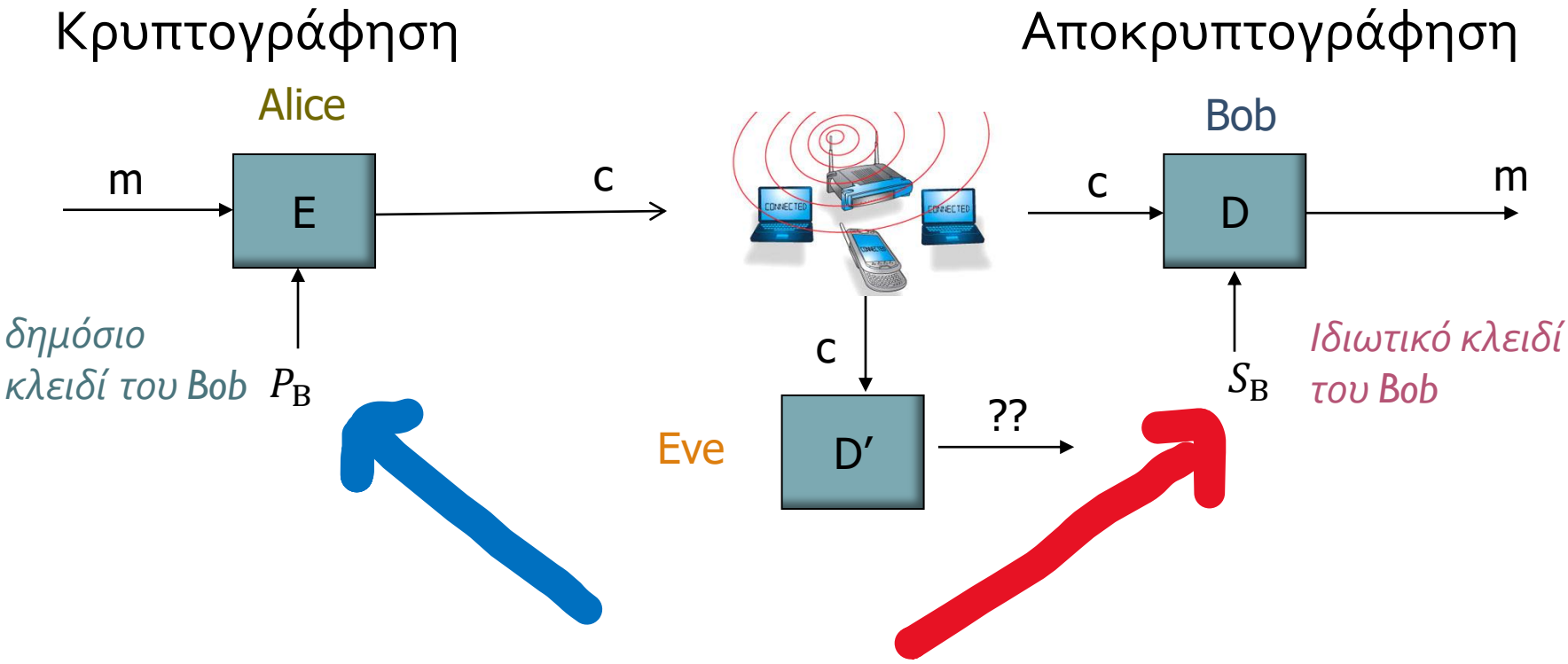
Ζητείται $x \leq p - 1$: $a = g^x \bmod p$

- *Εκτίμηση:* υπολογιστικά δύσκολο (όχι στο **P**)
- Λύνεται *αποδοτικά* με κβαντικό υπολογιστή

«ΠΥΛΏΝΕΣ» ΤΟΥ DHKE

- Υπολογιστική ευκολία της ύψωσης σε δύναμη (mod p) αριθμού χιλιάδων ψηφίων, με εκθέτη χιλιάδων ψηφίων
- Υπολογιστική ευκολία ελέγχου και εύρεσης πρώτων αριθμών με χιλιάδες ψηφία
- Υπολογιστική δυσκολία εύρεσης διακριτού λογαρίθμου αριθμού με χιλιάδες ψηφία αλλά και του απλούστερου προβλήματος DIFFIE-HELLMAN: (δοθέντων $g^a \bmod p$ και $g^b \bmod p$ να υπολογιστεί $g^{ab} \bmod p$)

ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ



- … με χρήση δημοσίου κλειδιού μαζί με *απόλυτα ιδιωτικό*, γνωστό στον παραλήπτη μόνο (κρυπτογραφία μονής κατεύθυνσης)

ΚΡΥΠ/ΦΙΑ ΔΗΜΟΣΟΥ ΚΛΕΙΔΙΟΥ / RSA

- Κρυπτογραφία δημοσίου κλειδιού: κατάργησε την ανάγκη ανταλλαγής κλειδιών! Στηρίζεται στην ύπαρξη συναρτήσεων μονής κατεύθυνσης.
- Συναρτήσεις μονής κατεύθυνσης (one-way functions): εύκολο να υπολογιστούν, δύσκολο να αντιστραφούν
- Κρυπτοσύστημα RSA [Rivest-Shamir-Adleman, 1977]
  - κρυπτογράφηση: $c = m^e \mod n$
  - αποκρυπτογράφηση: $m = c^d \mod n$
  - δημόσιο κλειδί: e, n
  - ιδιωτικό κλειδί: d

ΠΑΡΑΔΕΙΓΜΑ RSA [HTTP://NMICHAELS.ORG/RSA.PY]

- κρυπ/ση: $c = m^e \ mod\ n$ απκρ/ση: $m = c^d \ mod\ n$
- δημόσιο κλειδί (1ο μέρος) *n* =
  `d543be11021217e30589b41f796fac8f54a8905a4ddcd2007e2d00`
  `47d7b751a1aa60db5a080545a4ee2b33a2a119cc7aa3ff5b022d89`
  `54eeb5b72d1eec7cf40dfdc7947da9f49009c62be9d89fda3c7113`
  `7bbd009d3631bfa83bcde81a7bbc261890d2edd2fb20a4f0cb904b`
  `40bd5662c3c006634a7fcd7eae87a6d494e5fb5` (hex)
- δημόσιο κλειδί (2ο μέρος) e = `10001` (hex)
- ιδιωτικό κλειδί: *d* =
  `47b5fb04312ecb57d78a082c8151ff65547b49d108743678b663f3`
  `746feeee18d81523463327c84b786ba78515601c69081437c3e23e`
  `f4b6b2b0ad99d47e7c0228333da1594f774c8a73d4093f47663555`
  `7209945423cbd1e9b6a358f8254ed831c30d61f85cf57a49b8c7b1`
  `a21282d2fad548c12aa10f2ed0e5ccd5c7e32841` (hex)

Παραγοντοποιηση

- Δίνεται σύνθετος αριθμός n, βρείτε τους πρώτους παράγοντές του:

```
123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3

=

33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489

x

36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917
```

Παραγοντοποιηση

- *Εκτίμηση:* υπολογιστικά δύσκολο (όχι στο **P**)
- *Ευεπίλυτο με* κβαντικό υπολογιστή

«ΠΥΛΩΝΕΣ» ΤΟΥ RSA

- Υπολογιστική ευκολία της ύψωσης σε δύναμη (modulo p) αριθμού χιλιάδων ψηφίων, με εκθέτη χιλιάδων ψηφίων
- Υπολογιστική ευκολία ελέγχου και εύρεσης πρώτων αριθμών με χιλιάδες ψηφία
- Υπολογιστική ευκολία υπολογισμού αντιστρόφου a modulo n (a, n με χιλιάδες ψηφία) – μέσω αλγορίθμου Ευκλείδη!
- Υπολογιστική δυσκολία παραγοντοποίησης αριθμών με χιλιάδες ψηφία

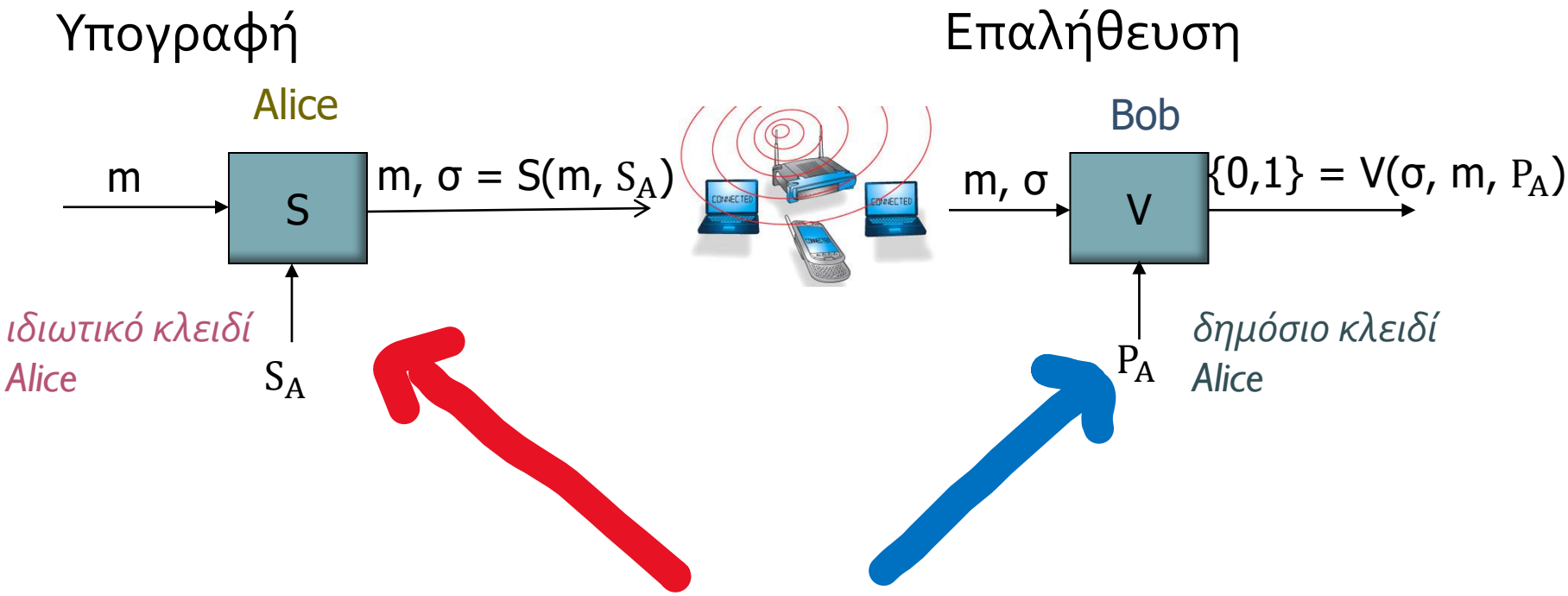
ΣΗΜΑΣΙΑ ΠΟΛΥΩΝΥΜΙΚΟΥ ΧΡΟΝΟΥ

- Έχει ταυτιστεί με την υπολογιστική ευκολία
- Επιτρέπει (συνήθως) την επίλυση πολύ μεγάλων «στιγμιοτύπων» (εισόδων)
- **Πρακτικά και «χοντρικά»:**
  - *αν μπορείς να το γράψεις μπορείς και να το υπολογίσεις!*

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΣΤΗΝ ΠΡΑΞΗ

- Συνήθης μέθοδος
  - Χρήση πρωτοκόλλων ταυτοποίησης για εγκαθίδρυση επικοινωνίας
  - Χρήση κρυπτογραφίας δημοσίου κλειδιού (π.χ. RSA ή DHKE) για ανταλλαγή ιδιωτικού συμμετρικού *κλειδιού συνεδρίας* (session key)
  - Χρήση συμμετρικής κρυπτογραφίας (π.χ. DES, AES) για ανταλλαγή δεδομένων
- Εφαρμογές σε: HTTPS, SSL/TLS, S-MIME, …

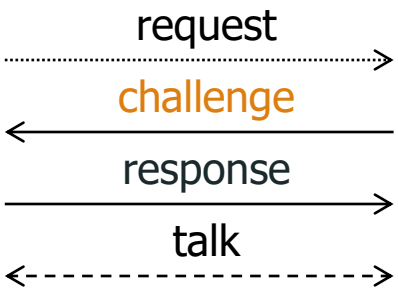
ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΥΠΟΓΡΑΦΕΣ



- … με χρήση δημοσίου κλειδιού, μαζί με *απόλυτα* ιδιωτικό, γνωστό στον υπογράφοντα μόνο

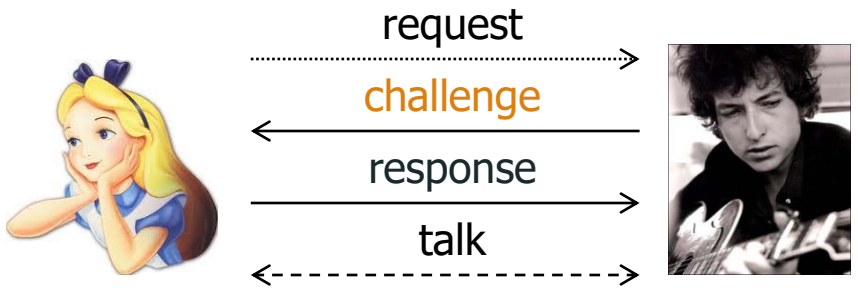
ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΠΡΩΤΟΚΟΛΛΑ

- Ταυτοποίηση / Πιστοποίηση

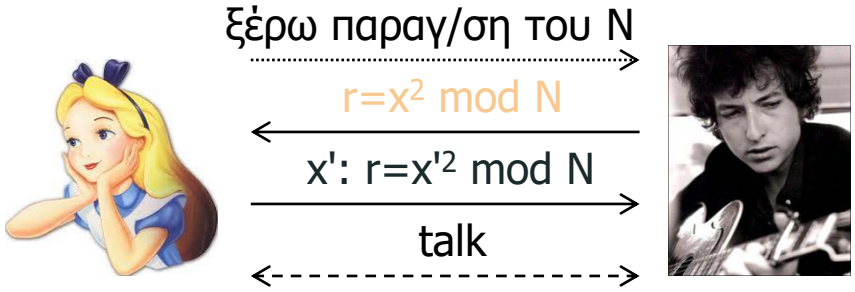


ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΠΡΩΤΟΚΟΛΛΑ

- Ταυτοποίηση / Πιστοποίηση

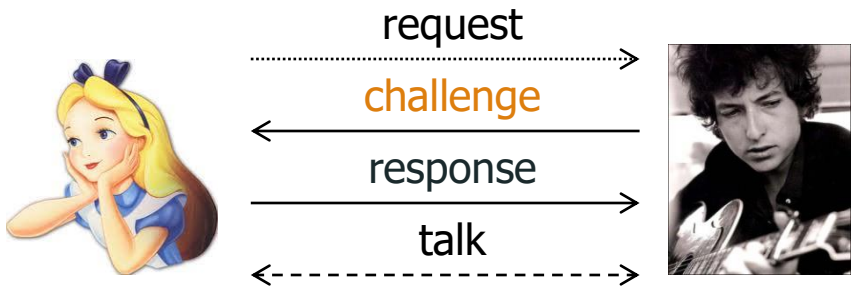


- Αποδείξεις γνώσης

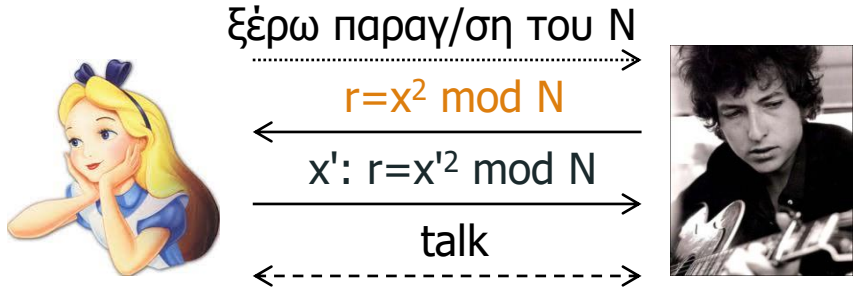


ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΠΡΩΤΟΚΟΛΛΑ

- Ταυτοποίηση / Πιστοποίηση



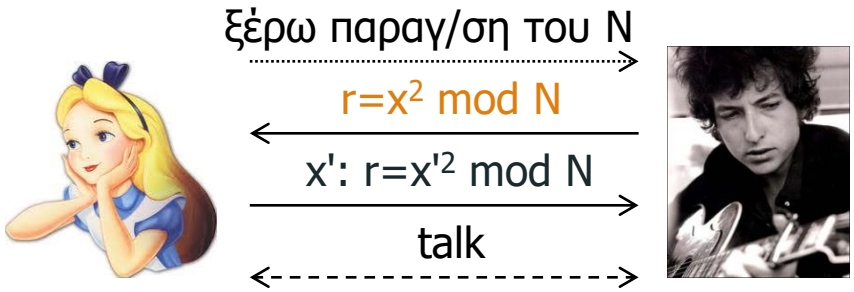
- Αποδείξεις γνώσης



… ακόμη και μηδενικής γνώσης! (πιο περίπλοκο)

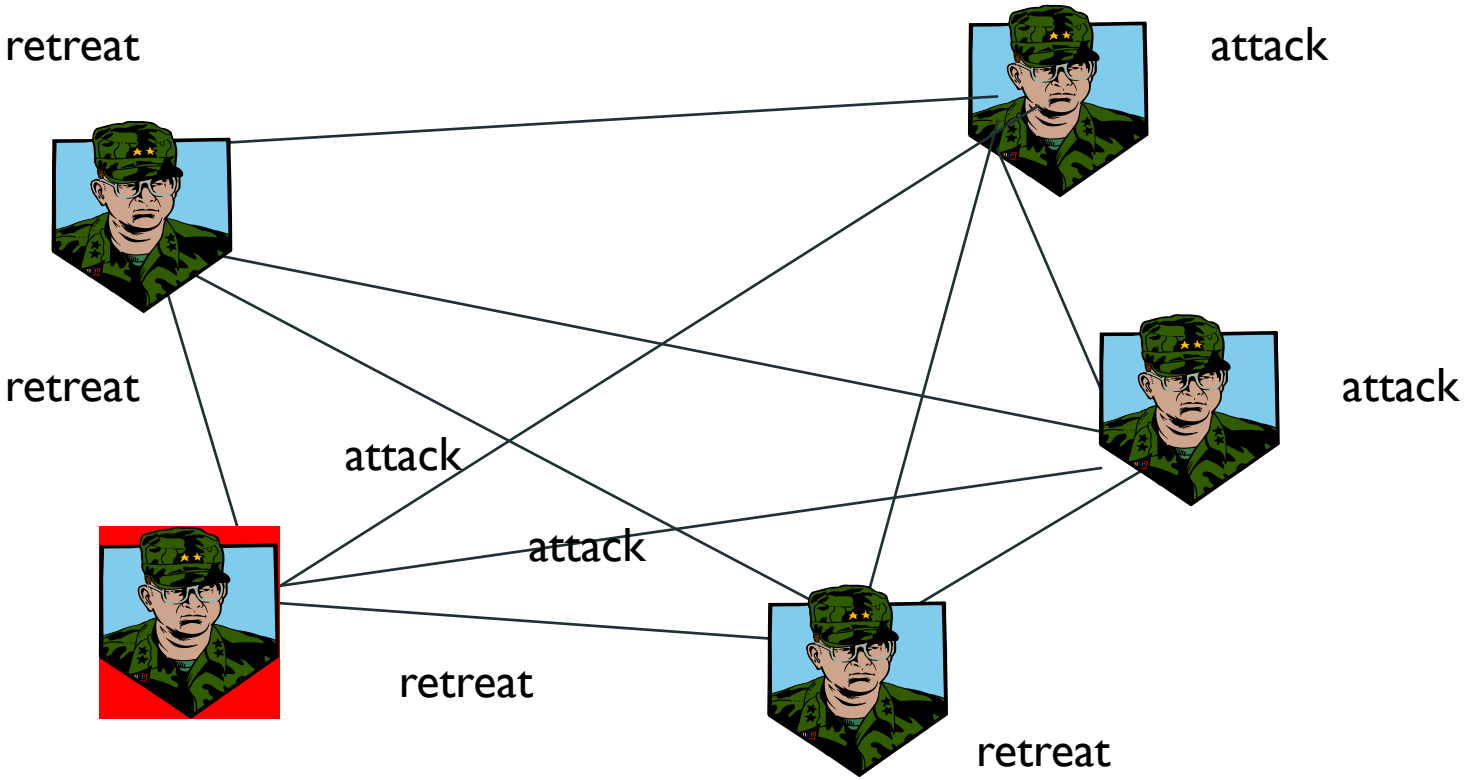
ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΠΡΩΤΟΚΟΛΛΑ

- Μη συνειδητή μεταφορά (oblivious transfer)

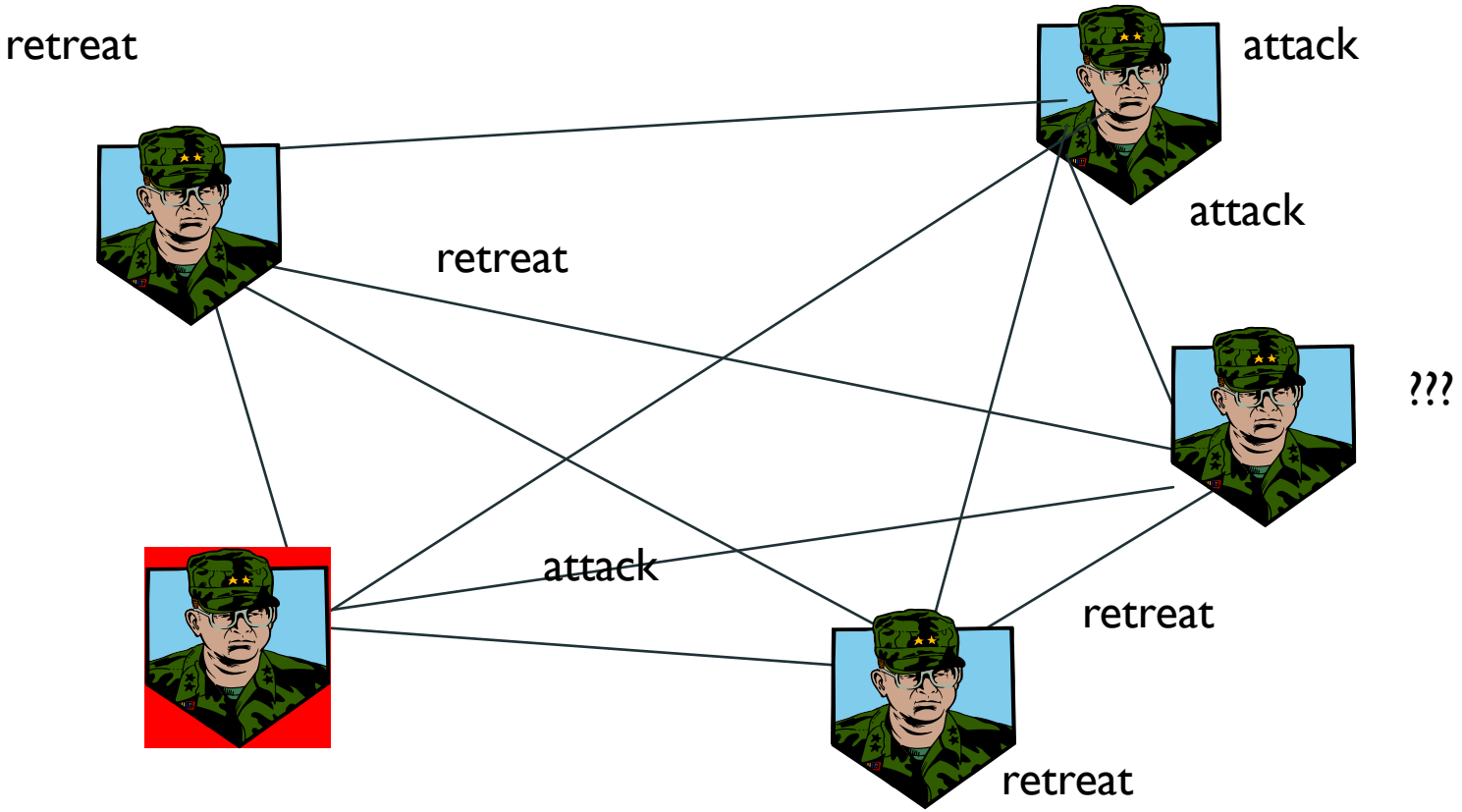


- Η Αλίκη δεν ξέρει αν ο Bob έμαθε κάτι ή όχι
- *Πολύ σημαντικό πρωτόκολλο!*

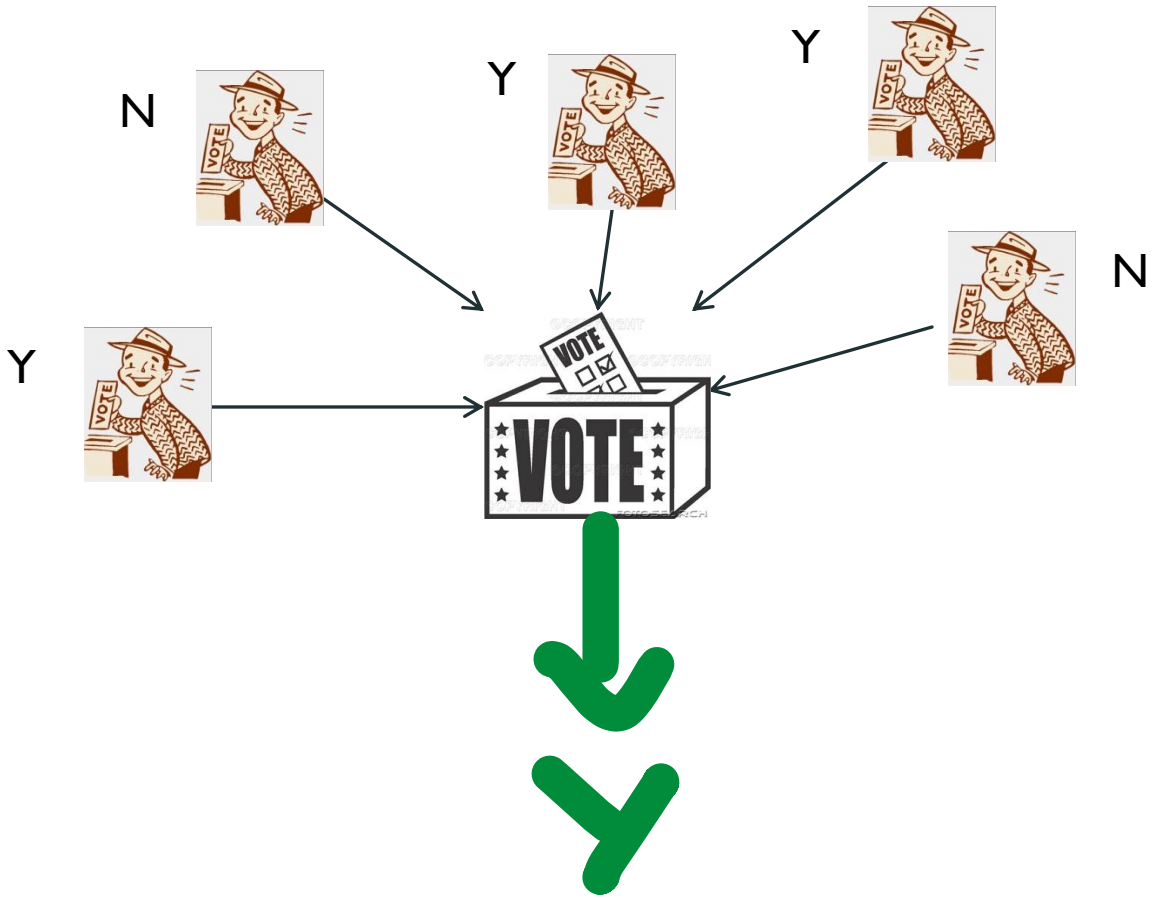
ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΒΥΖΑΝΤΙΝΕΣ ΕΠΙΘΕΣΕΙΣ / ΟΜΟΦΩΝΙΑ



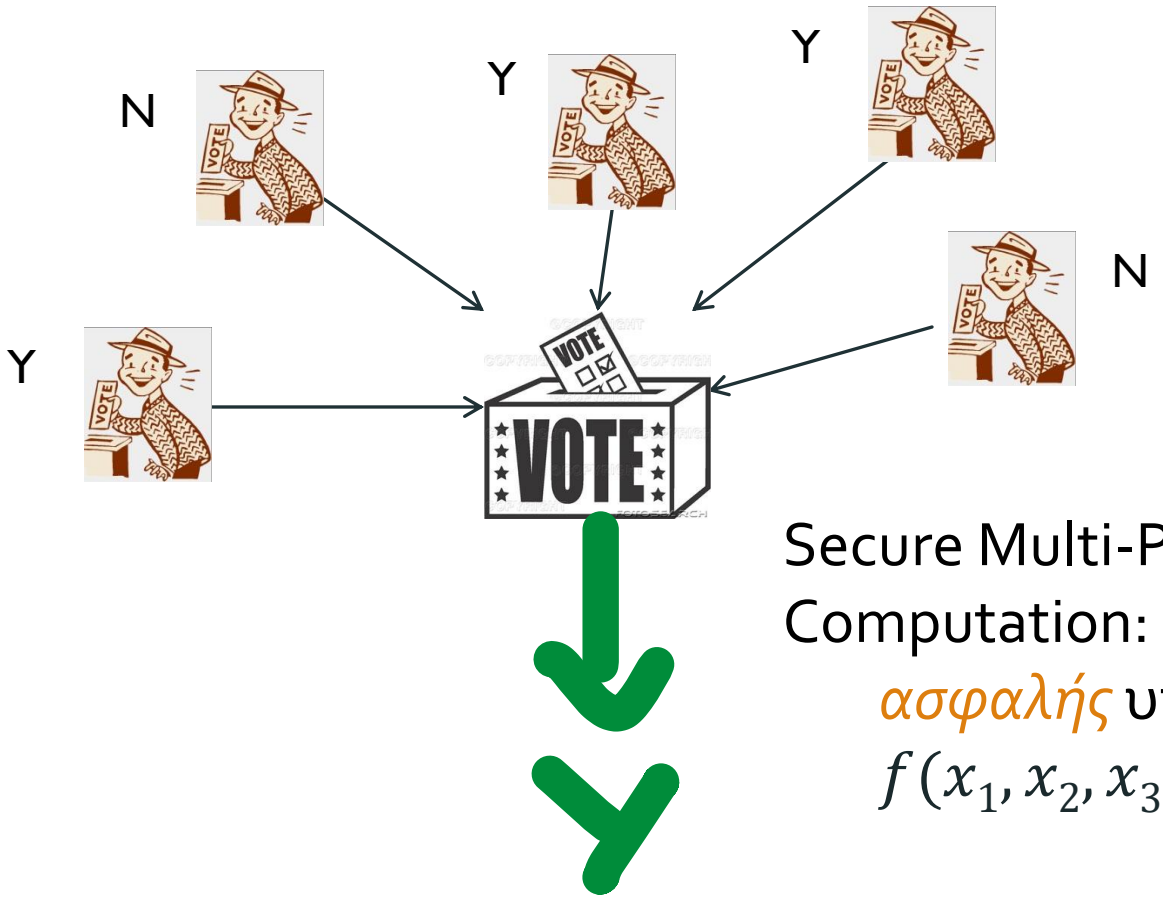
ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΒΥΖΑΝΤΙΝΕΣ ΕΠΙΘΕΣΕΙΣ / ΟΜΟΦΩΝΙΑ



ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΗΛ. ΨΗΦΟΦΟΡΙΕΣ



ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΗΛ. ΨΗΦΟΦΟΡΙΕΣ



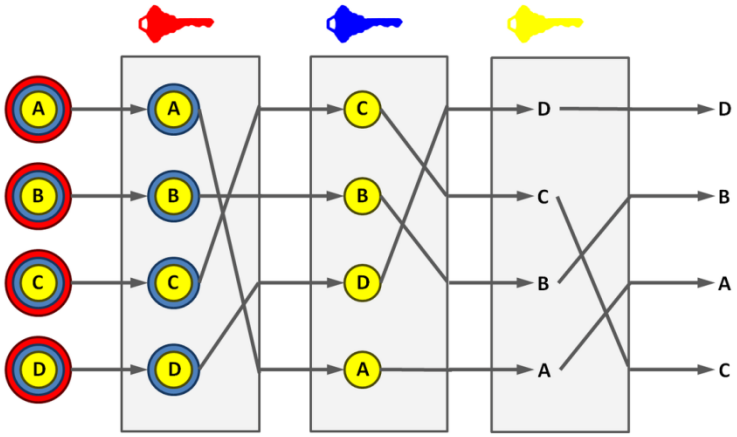
Secure Multi-Party Computation:

ασφαλής υπολογισμός

$f(x_1, x_2, x_3, x_4, x_5)$

ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΑΝΩΝΥΜΙΑ

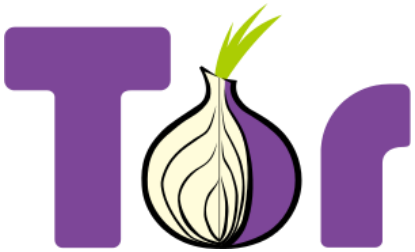
- Τεχνικές ανωνυμοποίησης
  - Mixnets



  - Blind signatures
    - *Ο υπογράφων υπογράφει «μεταμφιεσμένο» μήνυμα*

ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: ΑΝΩΝΥΜΙΑ

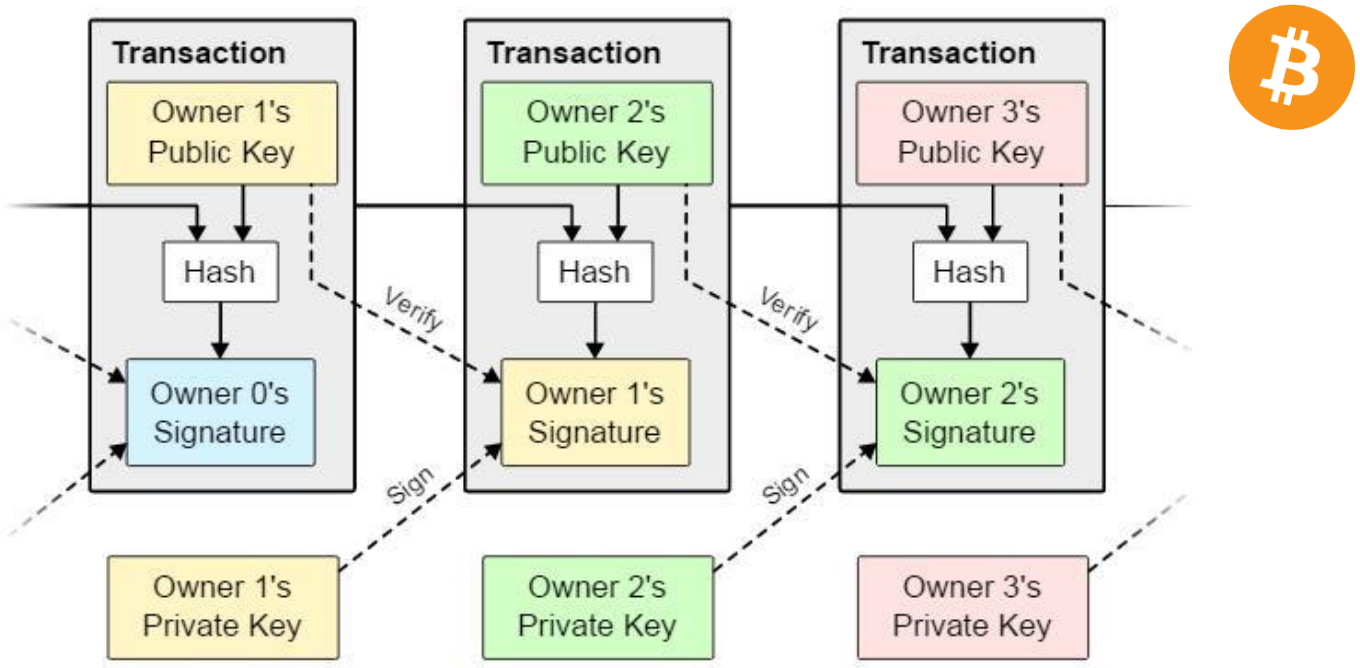
- **Tor**: ανώνυμη περιήγηση στο δίκτυο



- **OTR**: πιστοποιημένη ιδιωτική ανταλλαγή μηνυμάτων, με δυνατότητα αποποίησης (**deniability**) και **forward secrecy**

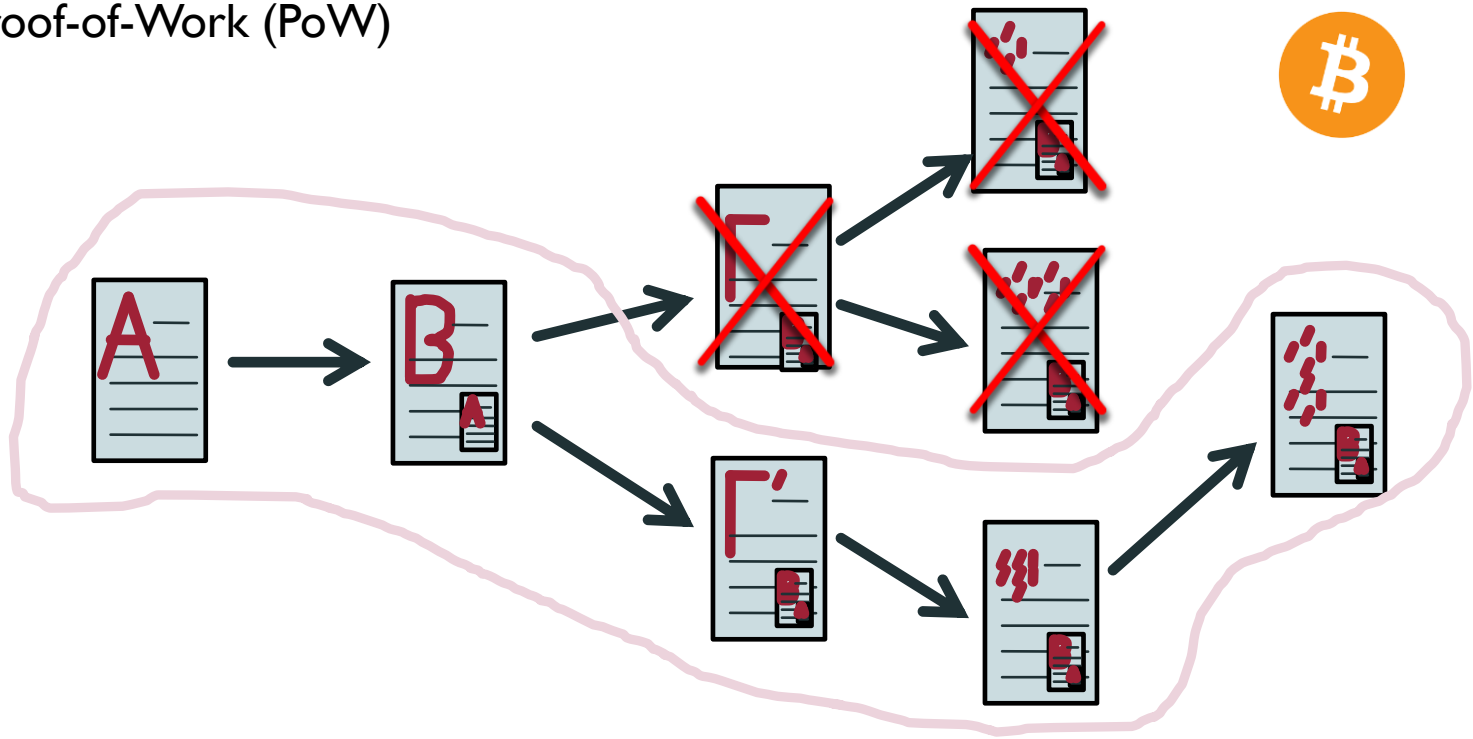
ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: BITCOIN

Bitcoin [Satoshi Nakamoto 2008]



ΜΙΑ ΠΡΩΤΗ ΜΑΤΙΑ: BITCOIN

Proof-of-Work (PoW)



ΣΤΟΧΟΙ ΤΟΥ ΜΑΘΗΜΑΤΟΣ

- Να εξοικειωθούμε με τις θεμελιώδεις κρυπτογραφικές λειτουργίες και τα πιο σημαντικά κρυπτοσυστήματα και πρωτόκολλα
- Να μπορούμε να αναλύσουμε τις ιδιότητές τους και την ασφάλειά τους, σε σχέση και με τις δυνατότητες του αντιπάλου
- Να μπορούμε να επιχειρηματολογήσουμε με αυστηρό τρόπο για τα παραπάνω

ΜΑΘΗΜΑΤΙΚΑ ΕΡΓΑΛΕΙΑ

- Θεωρία αριθμών
- Άλγεβρα (γραμμική και αφηρημένη)
- Πιθανότητες
- Υπολογιστική πολυπλοκότητα

Πολλά ενδιαφέροντα ανοιχτά προβλήματα και θέματα για παραπέρα έρευνα!