

ΥΠΟΛΟΓΙΣΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Εισαγωγή

Άρης Παγουρτζής – Στάθης Ζάχος

Σχολή ΗΜΜΥ ΕΜΠ

Διοικητικά του μαθήματος (2017-18)

- Διδάσκοντες
 - Στάθης Ζάχος
 - Άρης Παγουρτζής
 - Πέτρος Ποτίκας
- Βοηθοί διδασκαλίας
 - Παναγιώτης Γροντάς
 - Γιάννης Παπαϊωάννου
 - Δημήτρης Σακαβάλας
 - Αλέξανδρος Ζαχαράκης

Διοικητικά του μαθήματος

(2017-18)

- Ημέρες-ώρες
 - Τρίτη 17:15-19:00
 - Παρασκευή 16:00-18:00
- Ιστοσελίδα:
 - <http://www.corelab.ntua.gr/courses/crypto>
- Βαθμολογικό σχήμα:
 - Ασκήσεις (θεωρητικές / πρακτικές): 2 μονάδες
 - Εργασία (project): 1 μονάδα
 - Τελικό διαγώνισμα: 8 μονάδες (απαραίτητες 3)

Τι είναι η Κρυπτογραφία

- 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, ιδιωτικά data

Σημασία της Κρυπτογραφίας

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

Η ομορφιά της Κρυπτογραφίας

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

Προθέρμανση: ένα πρόβλημα

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

(αποτελείται από 9 διαφορετικά ψηφία)

Το πρόβλημα του 2^{29}

Πόσες πράξεις χρειαζόμαστε;

Γίνεται καλύτερα;

Το πρόβλημα του 2^{29}

Γίνεται χωρίς να υπολογίσουμε τον αριθμό;

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

Μια πρώτη ματιά: ιδιωτικότητα

Κρυπτογράφηση

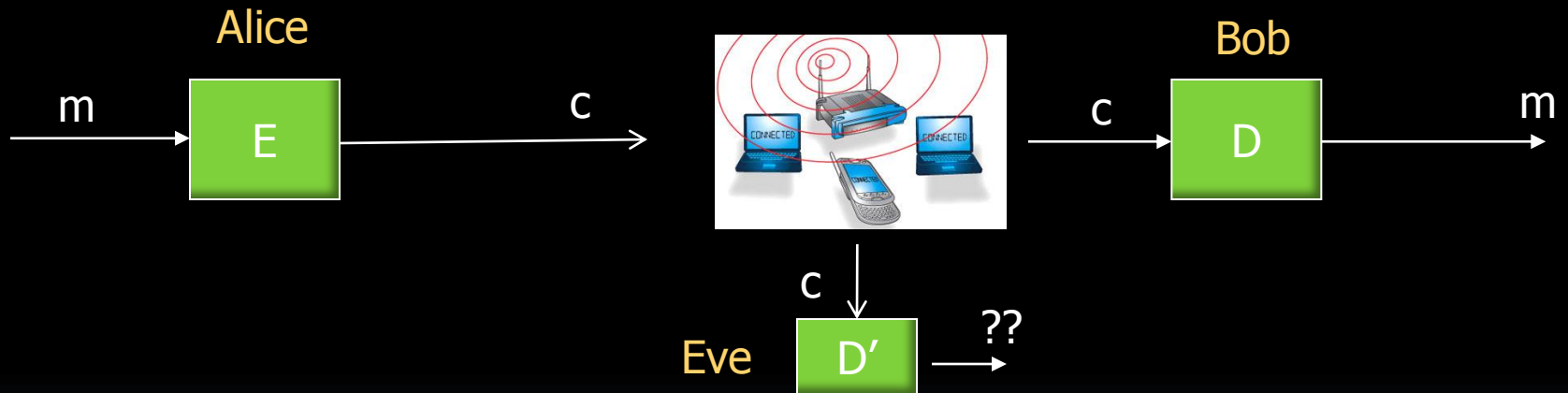
Αποκρυπτογράφηση



Μια πρώτη ματιά: ιδιωτικότητα

Κρυπτογράφηση

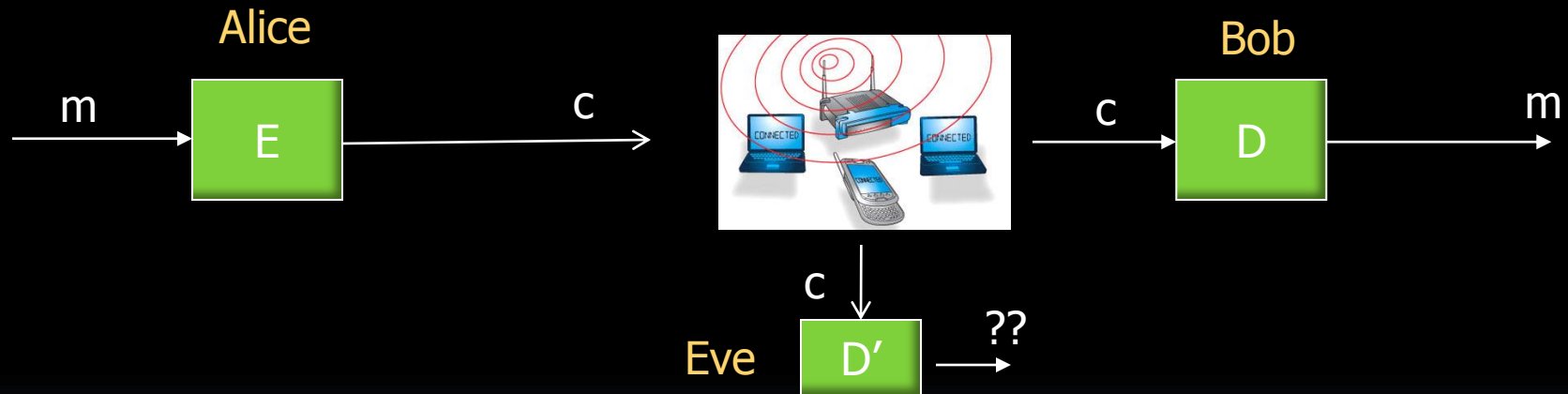
Αποκρυπτογράφηση



Μια πρώτη ματιά: ιδιωτικότητα

Κρυπτογράφηση

Αποκρυπτογράφηση

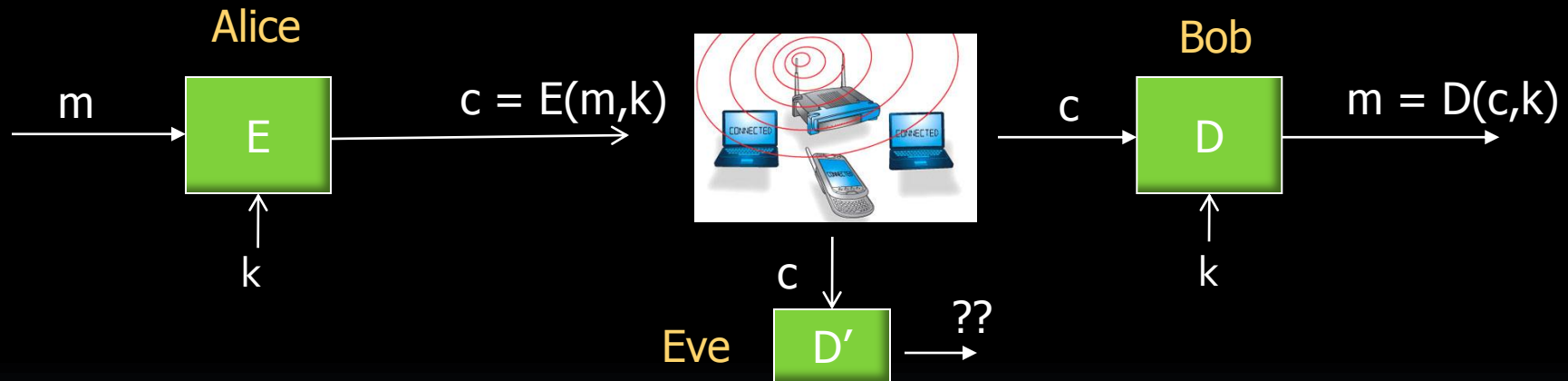


- ... με χρήση *κοινού ιδιωτικού κλειδιού* (συμμετρική κρυπτογραφία)

Μια πρώτη ματιά: ιδιωτικότητα

Κρυπτογράφηση

Αποκρυπτογράφηση

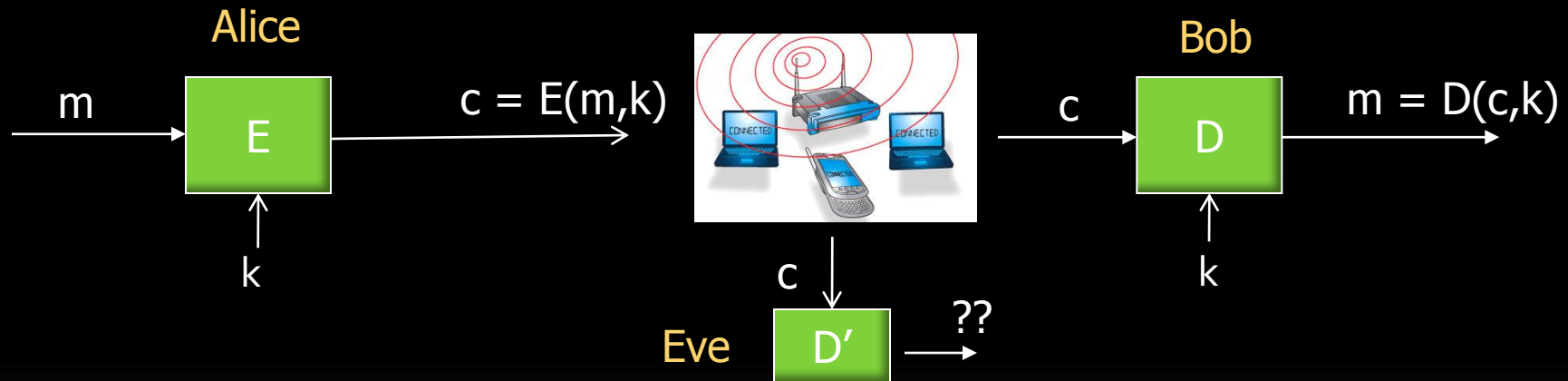


- ... με χρήση *κοινού ιδιωτικού κλειδιού* (συμμετρική κρυπτογραφία)

Μια πρώτη ματιά: ιδιωτικότητα

Κρυπτογράφηση

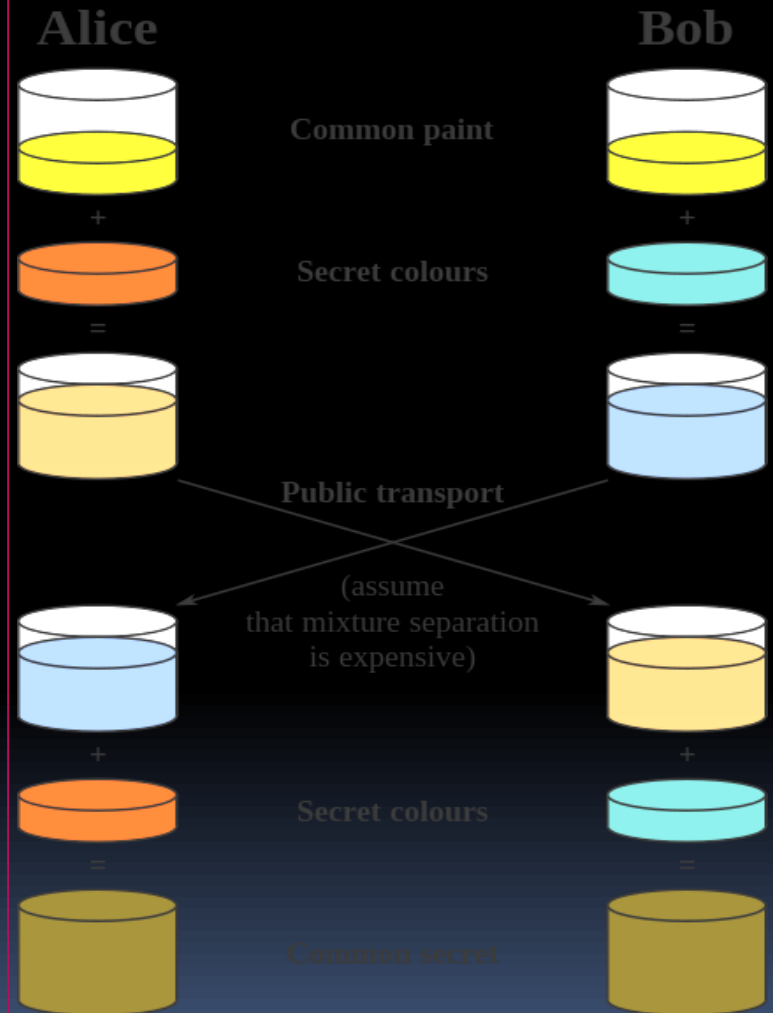
Αποκρυπτογράφηση



- ... με χρήση *κοινού ιδιωτικού κλειδιού* (συμμετρική κρυπτογραφία)
- *ανταλλαγή κλειδιού?*

Λύση: Diffie-Hellman Key Exchange

- Επιλέγονται: πρώτος p , και γεννήτορας g της $Z_p^* = \{1, \dots, p-1\}$, γνωστοποιούνται σε A και B.
- $B \rightarrow A$: $b^* = g^b \text{ mod } p$
(b : ιδιωτικό κλειδί του B)
- $A \rightarrow B$: $a^* = g^a \text{ mod } p$
(a : ιδιωτικό κλειδί της A)
- A: $K = (b^*)^a \text{ mod } p = g^{ba} \text{ mod } p$
- B: $K = (a^*)^b \text{ mod } p = g^{ab} \text{ mod } p$
- 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 $Z_p^* = \{1, \dots, p-1\}$ και $a \in Z_p^*$. Ζητείται $x \leq p-1$:

$$a = g^x \pmod{p}$$

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

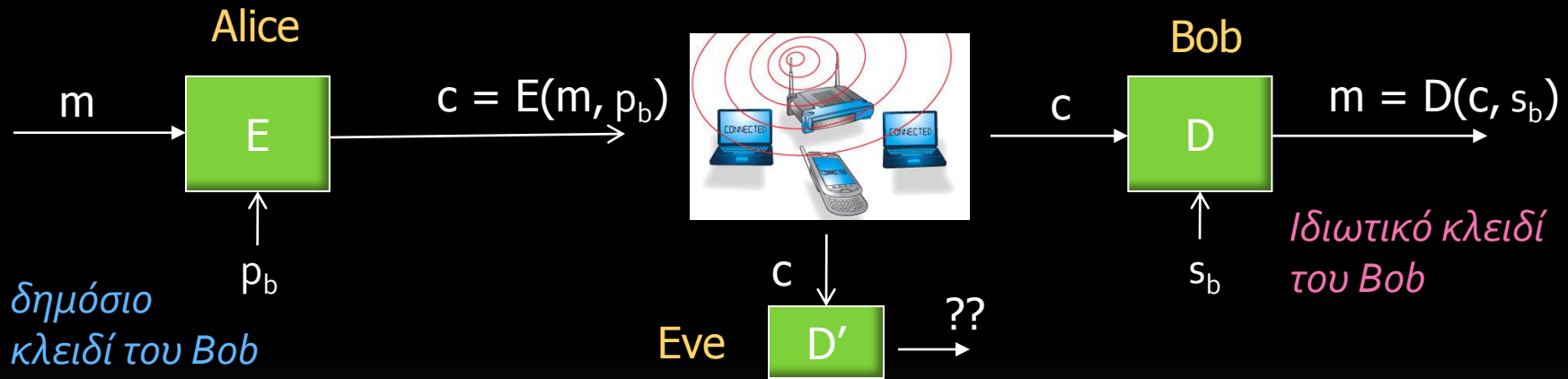
«Πυλώνες» του DHKE

- ❑ Υπολογιστική ευκολία της **ύψωσης σε δύναμη** ($\text{mod } p$) 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 $g^a \text{ mod } p$ και $g^b \text{ mod } p$ να υπολογιστεί $g^{ab} \text{ mod } p$)

2^η λύση: δημόσιο κλειδί

Κρυπτογράφηση

Αποκρυπτογράφηση



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

Κρυπ/φία δημοσίου κλειδιού / RSA

- Κρυπτογραφία **δημοσίου κλειδιού**: κατέργησε 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: $c = m^e \bmod n$
 - αποκρυπτογράφηση: $m = c^d \bmod n$
 - δημόσιο κλειδί: e, n
 - ιδιωτικό κλειδί: d

Παράδειγμα RSA

[<http://nmichaels.org/rsa.py>]

- κρυπ/ση: $c = m^e \bmod n$ απκρ/ση: $m = c^d \bmod n$
- δημόσιο κλειδί (1^ο μέρος) $n =$
d543be11021217e30589b41f796fac8f54a8905a4ddcd2007e2d0047d7b75
1a1aa60db5a080545a4ee2b33a2a119cc7aa3ff5b022d8954eeb5b72d1eec
7cf4odfdc7947dagf49009c62begd89fda3c71137bbd009d3631bfa83bcde
81a7bbc261890d2edd2fb20a4focb904b4obd5662c3c006634a7fcd7eae8
7a6d494e5fb5 (hex)
- δημόσιο κλειδί (2^ο μέρος) $e = 10001$ (hex)
- ιδιωτικό κλειδί: $d =$
47b5fbo4312ecb57d78a082c8151ff65547b49d108743678b663f3746feeee
18d81523463327c84b786ba78515601c69081437c3e23ef4b6b2boad99d4
7e7c0228333da1594f774c8a73d4093f476635557209945423cbd1e9b6a35
8f8254ed831c30d61f85cf57a49b8c7b1a21282d2fad548c12aa1of2edoe5c
cd5c7e32841 (hex)

ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ

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

123018668453011775513049495838496272077285356959533479219732245215172
640050726365751874520219978646938995647494277406384592519255732630345
373154826850791702612214291346167042921431160222124047927473779408066
5351419597459856902143413

=

33478071698956898786044169848212690817704794983713768568912431
388982883793878002287614711652531743087737814467999489

x

36746043666799590428244633799627952632279158164343087642676032
283815739666511279233373417143396810270092798736308917

ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ

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

«Πυλώνες» του RSA

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

Σημασία πολυωνυμτικού χρόνου

- ❑ Έχει ταυτιστεί με την υπολογιστική ευκολία
- ❑ Επιτρέπει (συνήθως) την επίλυση πολύ μεγάλων «στιγμιοτύπων» (εισόδων)
- ❑ Πρακτικά και «χοντρικά»:

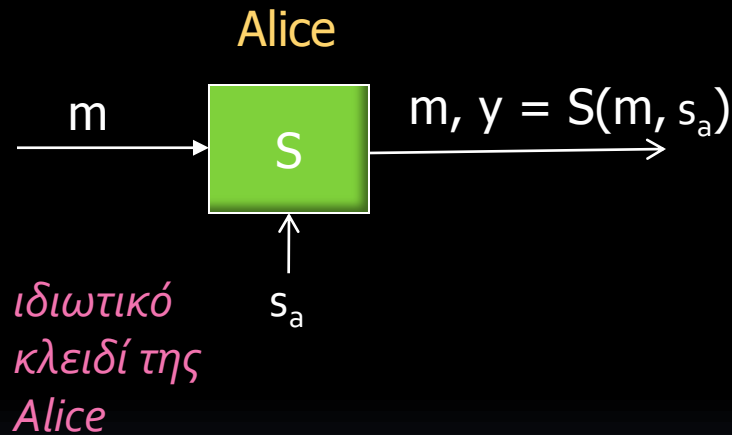
αν μπορείς να το γράψεις μπορείς και να το υπολογίσεις!

Ιδιωτικότητα στην πράξη

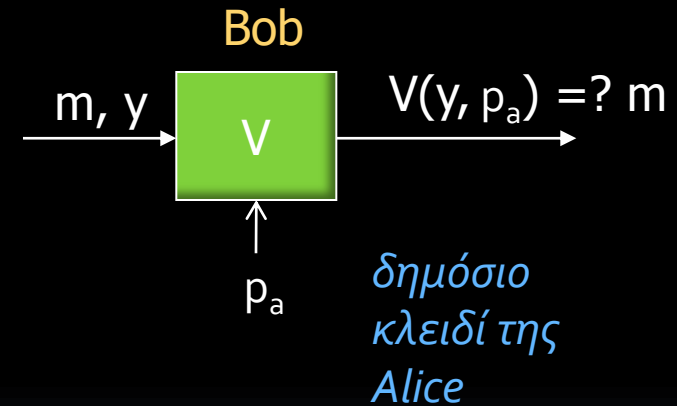
- Συνήθης μέθοδος
 - Χρήση πρωτοκόλλων ταυτοποίησης για εγκαθίδρυση επικοινωνίας
 - Χρήση κρυπτογραφίας δημοσίου κλειδιού (π.χ. **RSA** ή **DHKE**) για ανταλλαγή ιδιωτικού συμμετρικού *κλειδιού συνεδρίας* (session key)
 - Χρήση συμμετρικής κρυπτογραφίας (π.χ. **DES**, **AES**) για ανταλλαγή δεδομένων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

Μια πρώτη ματιά: Υπογραφές

Υπογραφή



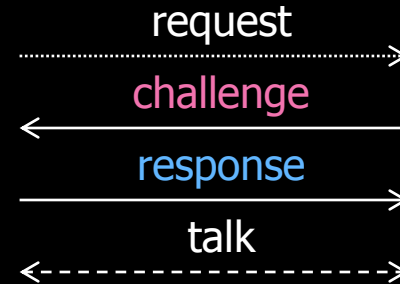
Επαλήθευση



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

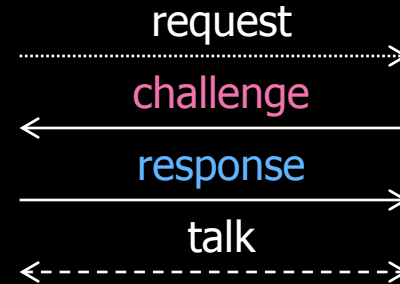
Μια πρώτη ματιά: πρωτόκολλα

- Ταυτοποίηση / Πιστοποίηση

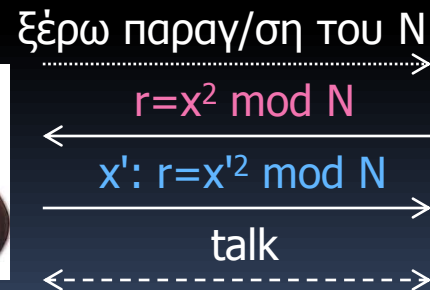


Μια πρώτη ματιά: πρωτόκολλα

- Ταυτοποίηση / Πιστοποίηση

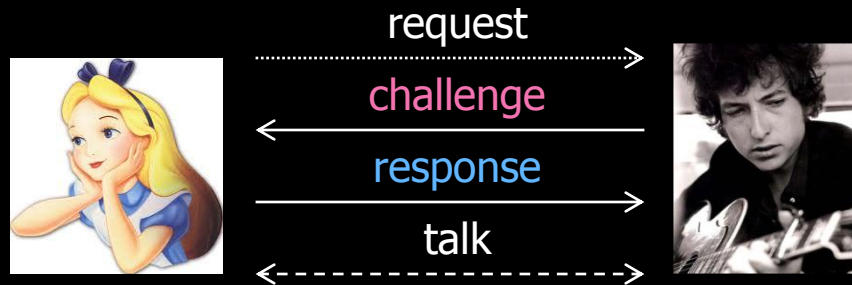


- Αποδείξεις γνώσης

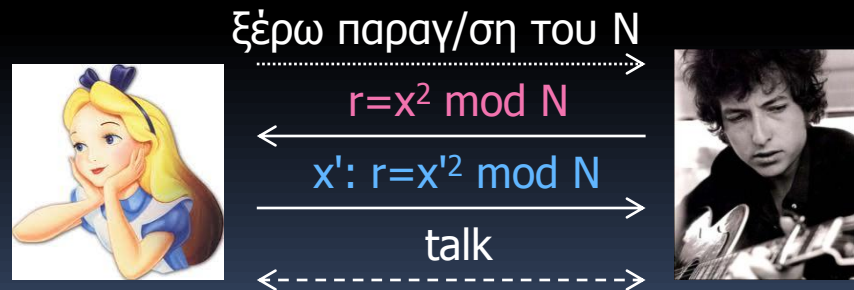


Μια πρώτη ματιά: πρωτόκολλα

- Ταυτοποίηση / Πιστοποίηση



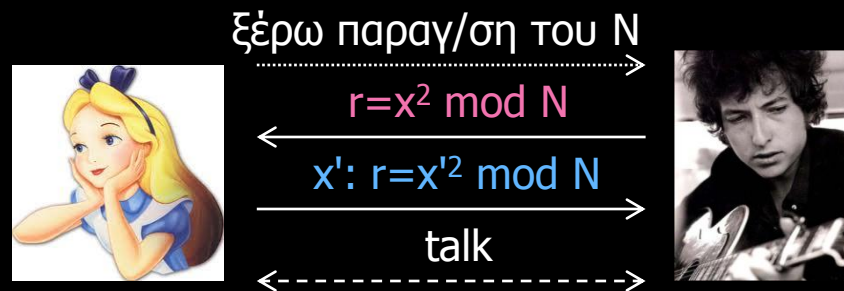
- Αποδείξεις γνώσης



... ακόμη και μηδενικής γνώσης! (πιο περίπλοκο)

Μια πρώτη ματιά: πρωτόκολλα

- Μη συνειδητή μεταφορά (oblivious transfer)



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

Μια πρώτη ματιά: πρωτόκολλα

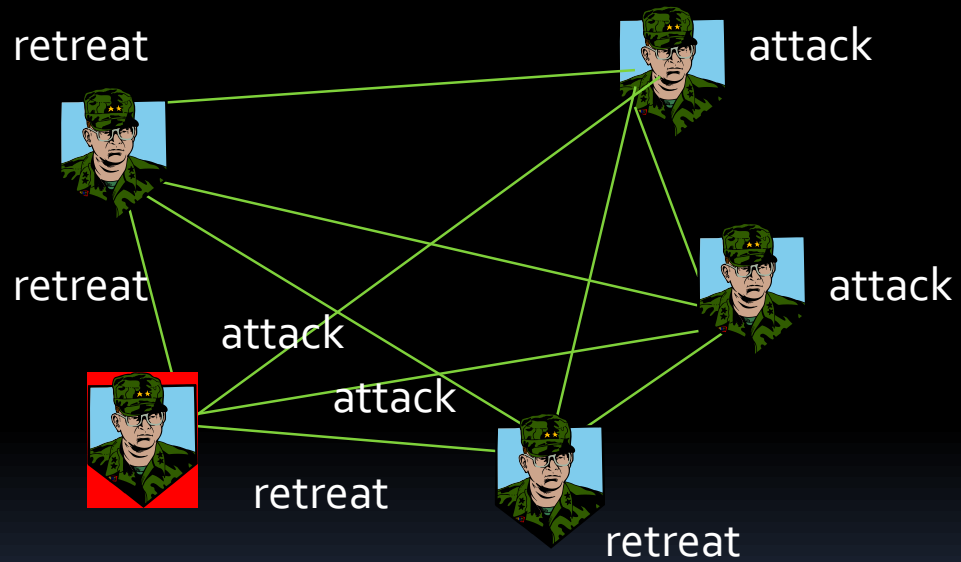
- Tor: ανώνυμη περιήγηση στο δίκτυο



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

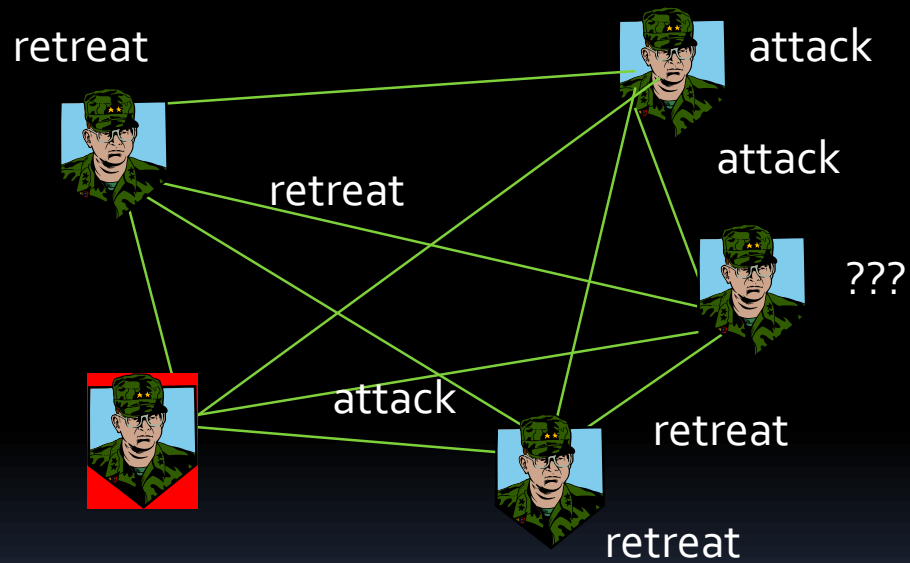
Μια πρώτη ματιά: πρωτόκολλα

- Βυζαντινοί στρατηγοί



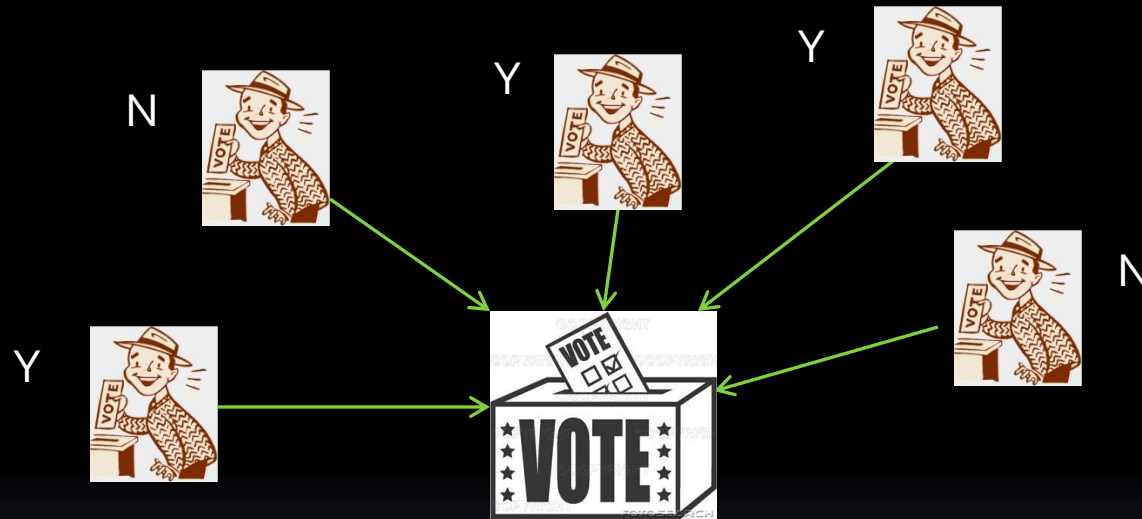
Μια πρώτη ματιά: πρωτόκολλα

- Βυζαντινοί στρατηγοί



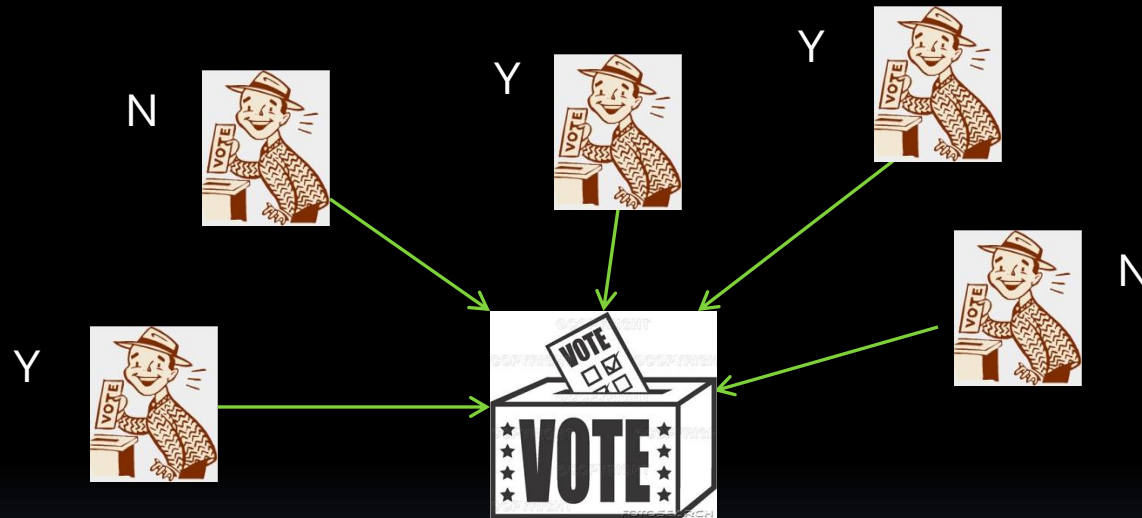
Μια πρώτη ματιά: πρωτόκολλα

- Ηλεκτρονικές ψηφοφορίες



Μια πρώτη ματιά: πρωτόκολλα

- Ηλεκτρονικές ψηφοφορίες

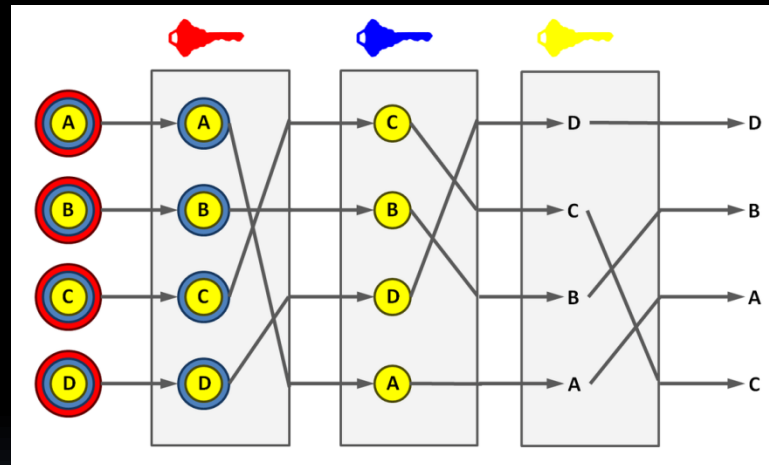


- Secure Multi-Party Computation:
 - ασφαλής υπολογισμός $f(x_1, x_2, x_3, x_4, x_5)$

Μια πρώτη ματιά: πρωτόκολλα

- Τεχνικές ανωνυμοποίησης

- Mixnets

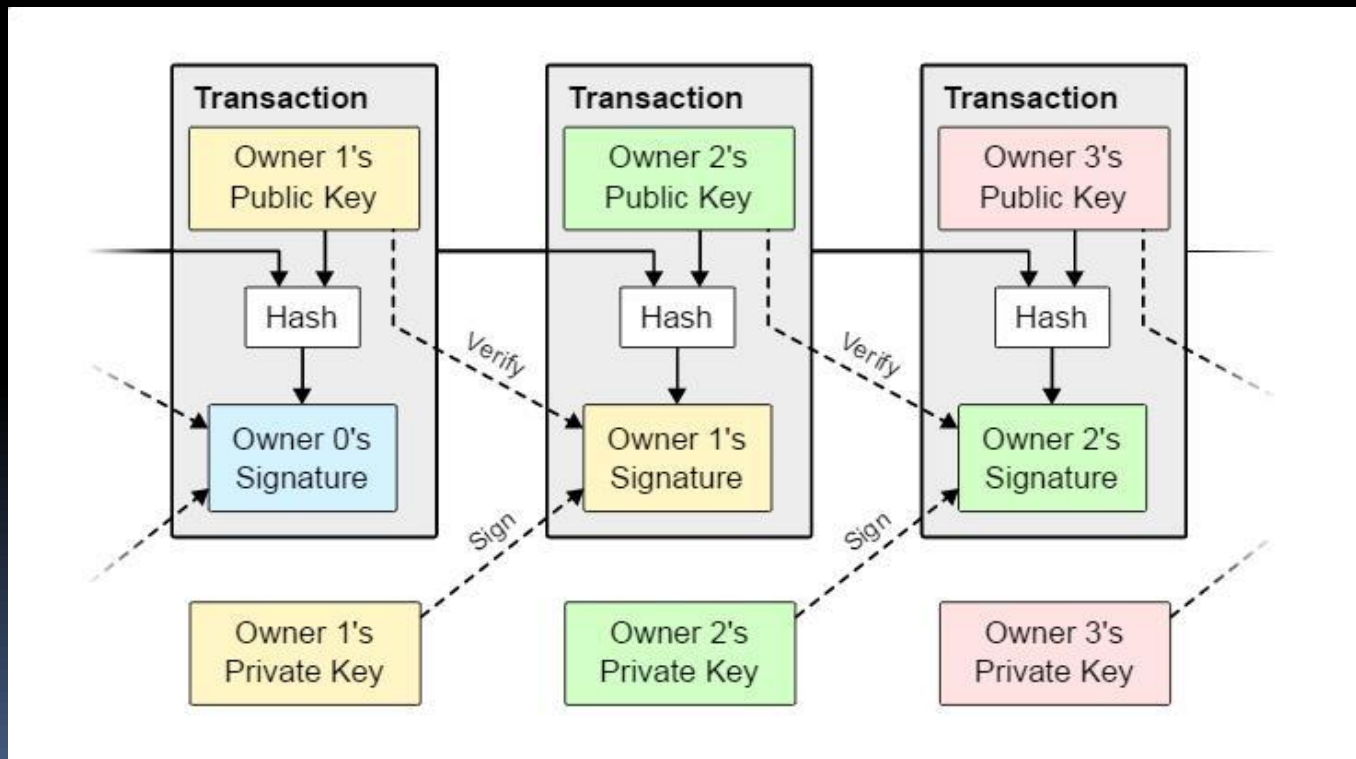


- Blind signatures

- *Ο υπογράφων υπογράφει «μεταμφιεσμένο» μήνυμα*

Μια πρώτη ματιά: πρωτόκολλα

- Bitcoin [Satoshi Nakamoto 2008]



Στόχοι του μαθήματος

- 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

Μαθηματικά εργαλεία

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

Πολλά ενδιαφέροντα ανοιχτά προβλήματα και θέματα για περαιτέρω έρευνα!