# ΥΠΟΛΟΓΙΣΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

## Εισαγωγή

*Άρης Παγουρτζής – Στάθης Ζάχος*
Σχολή ΗΜΜΥ ΕΜΠ

# Διοικητικά του μαθήματος (2019-20)

- Διδάσκοντες
  - Στάθης Ζάχος
  - Άρης Παγουρτζής
  - Πέτρος Ποτίκας
- Βοηθοί διδασκαλίας
  - Παναγιώτης Γροντάς
  - Γιάννης Παπαϊωάννου
  - Θωμάς Σουλιώτης

# Διοικητικά του μαθήματος (2019-20)

- Ημέρες-ώρες
  - Τρίτη 11:45-14:30
  - Παρασκευή 16:15-17:00
- 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 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 (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 ομορφιά της Κρυπτογραφίας

- 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!

# 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 πλήρως τον αριθμό;

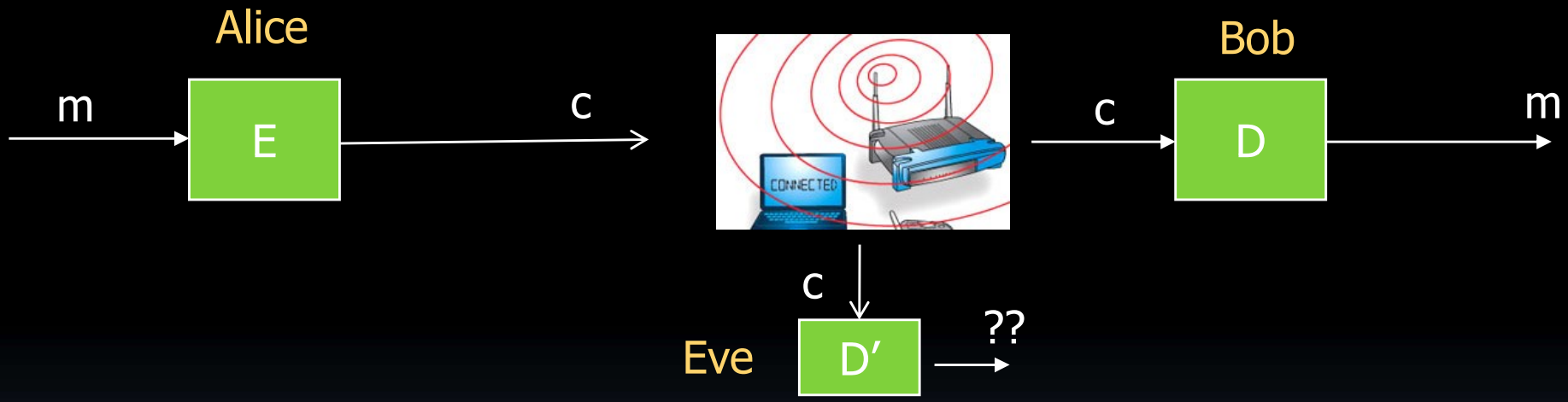
( ερώτηση από βιβλίο προετοιμασίας για συνεντεύξεις σε 'quant jobs' )

# Μια πρώτη ματιά: ιδιωτικότητα

Κρυπτογράφηση Αποκρυπτογράφηση

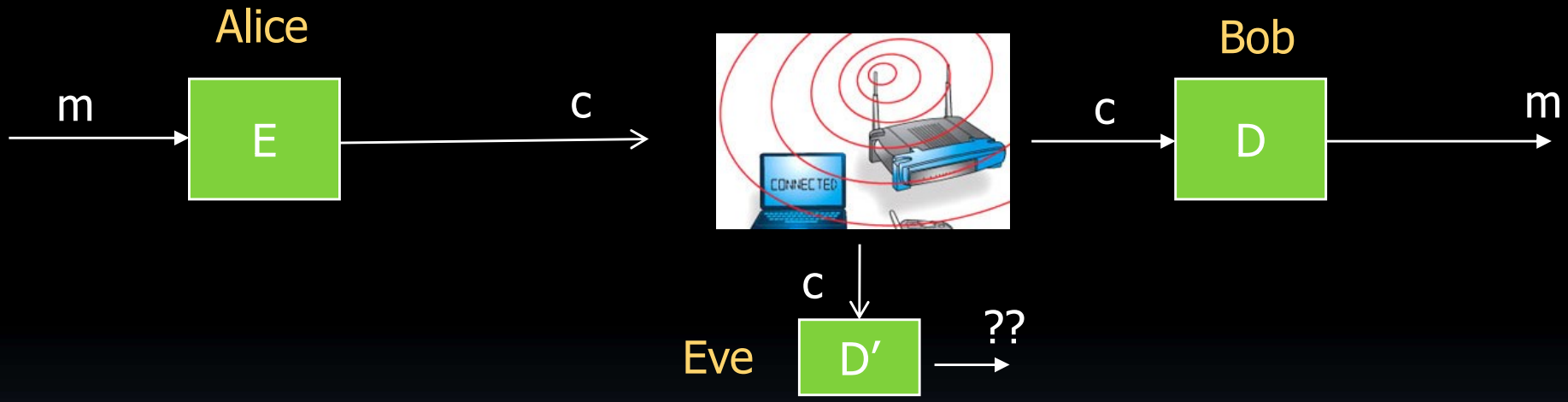
# Μια πρώτη ματιά: ιδιωτικότητα

Κρυπτογράφηση Αποκρυπτογράφηση



# Μια πρώτη ματιά: ιδιωτικότητα

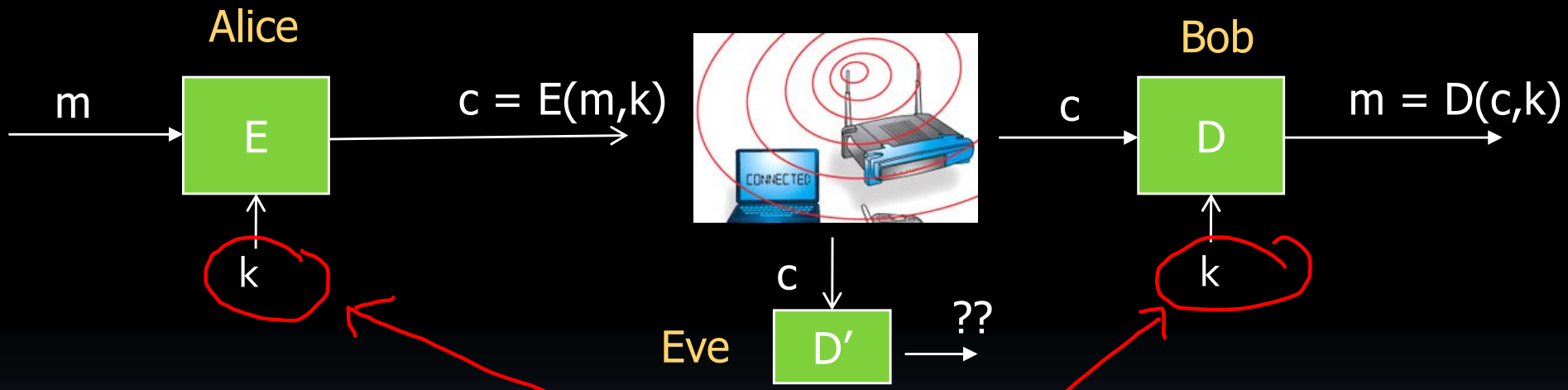
Κρυπτογράφηση Αποκρυπτογράφηση




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

# Μια πρώτη ματιά: ιδιωτικότητα

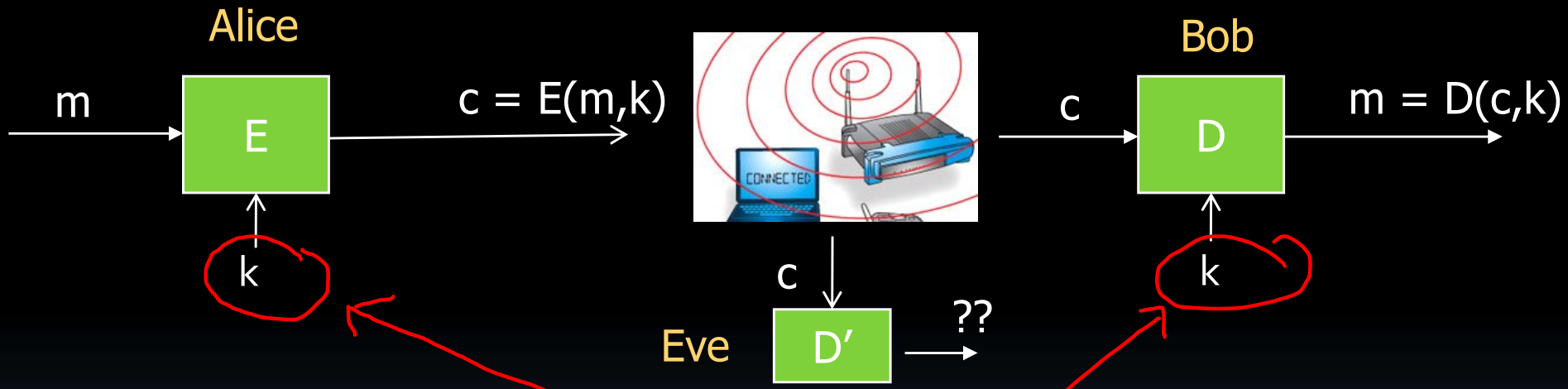
Κρυπτογράφηση Αποκρυπτογράφηση




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

# Μια πρώτη ματιά: ιδιωτικότητα

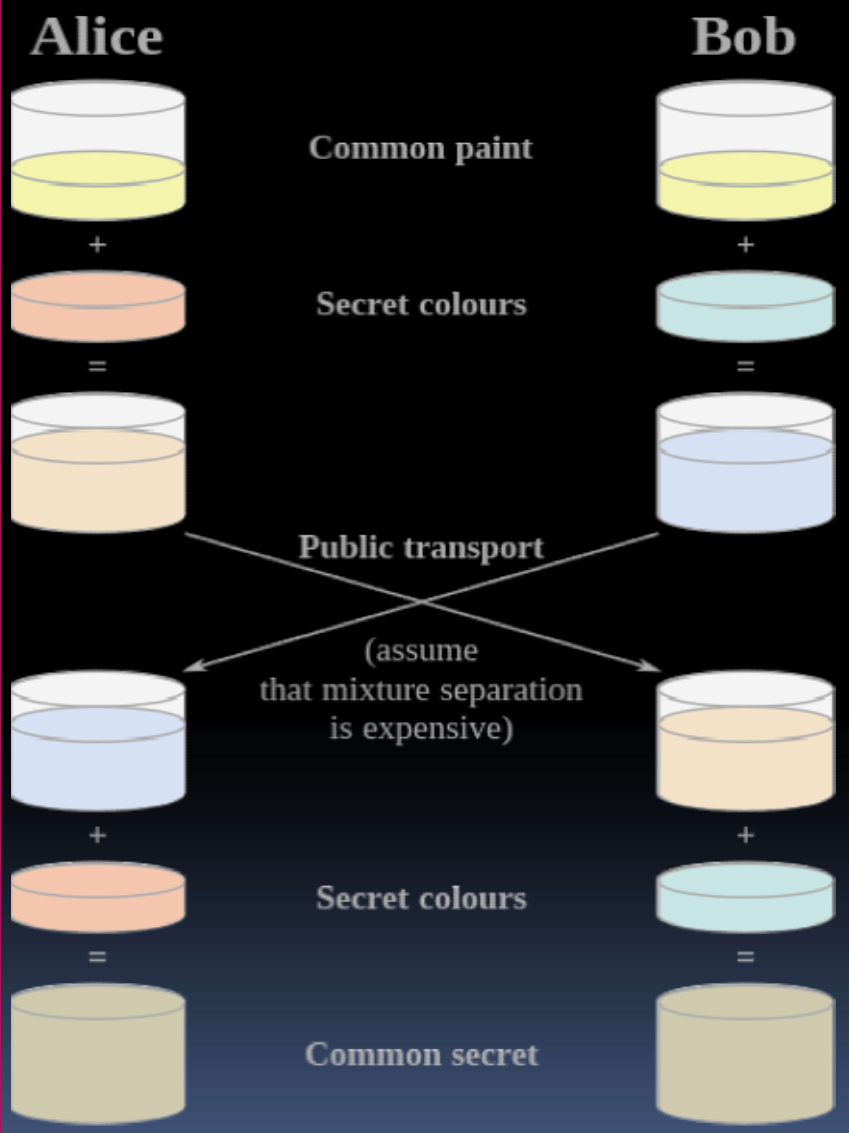
Κρυπτογράφηση Αποκρυπτογράφηση




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

# Λύση: Diffie-Hellman Key Exchange

- Επιλέγονται: πρώτος $p$, και γεννήτορας $g$ της $Z^*_p = \{1,..,p-1\}$, γνωστοποιούνται σε Α και Β.
- Β $\rightarrow$ Α: $b^* = g^b \bmod p$
  ($b$: ιδιωτικό κλειδί του Β)
- Α $\rightarrow$ Β: $a^* = g^a \bmod p$
  ($a$: ιδιωτικό κλειδί της Α)
- Α: $K = (b^*)^a \bmod p = g^{ba} \bmod p$
- Β: $K = (a^*)^b \bmod p = g^{ab} \bmod p$
- 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 $Z^*_p = \{1, \ldots, p-1\}$ και $\boldsymbol{a} \in Z^*_p$. Ζητείται $\boldsymbol{x} \leq p-1$:

$$a = g^x \bmod p$$

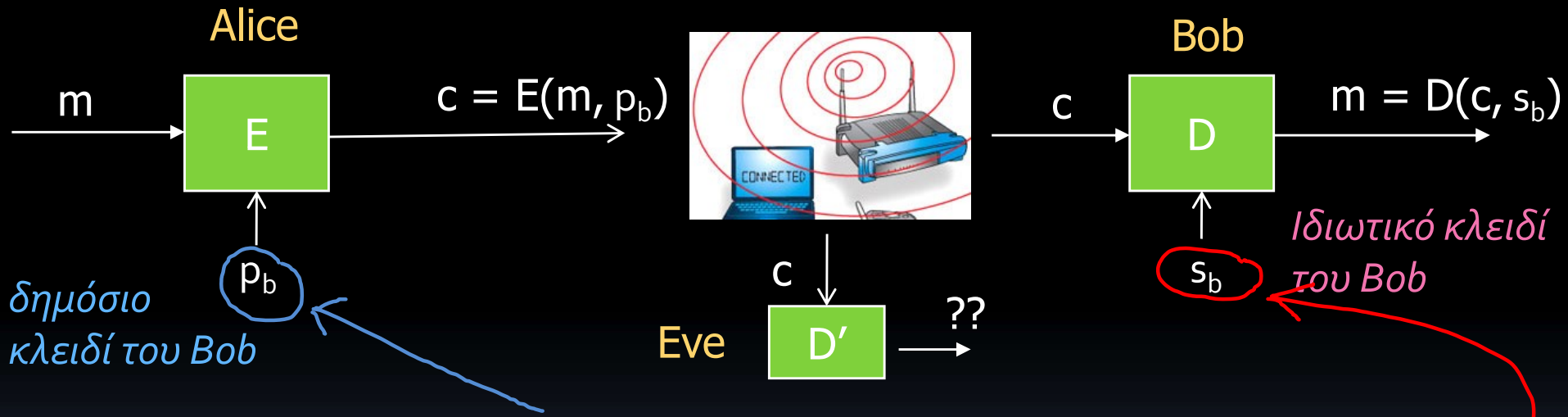
- *Εκτίμηση:* υπολογιστικά δύσκολο (όχι στο **P**)
- Λύνεται *αποδοτικά* με κβαντικό υπολογιστή

# «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 $g^{ab} \bmod p$ )

# 2η λύση: δημόσιο κλειδί

Κρυπτογράφηση Αποκρυπτογράφηση




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

# Κρυπ/φία δημοσίου κλειδιού / 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: $d$

# Παράδειγμα RSA [http://nmichaels.org/rsa.py]

- κρυπ/ση: $c = m^e \bmod n$ απκρ/ση: $m = c^d \bmod n$
- δημόσιο κλειδί (1ο μέρος) $n$ = d543be1102121 7e30589b41f796fac8f54a8905a4ddcd2007e2d0047d7b751a1aa60db5a080545a4ee2b33a2a119cc7aa3ff5b022d8954eeb5b72d1eec7cf40dfdc7947da9f49009c62be9d89fda3c71137bbd009d3631bfa83bcde81a7bbc261890d2edd2fb20a4focb904b40bd5662c3c006634a7fcd7eae87a6d494e5fb5 (hex)
- δημόσιο κλειδί (2ο μέρος) $e$ = 10001 (hex)
- ιδιωτικό κλειδί: $d$ = 47b5fb04312ecb57d78a082c8151ff65547b49d108743678b663f3746feeee18d81523463327c84b786ba7851560 1c69081437c3e23ef4b6b2b0ad99d47e7c0228333da1594f774c8a73d4093f476635557209945423cbd1e9b6a358f8254ed831c30d61f85cf57a49b8c7b1a21282d2fad548c12aa10f2ed0e5ccd5c7e32841 (hex)

# Παραγοντοποιηση

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

  1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

  =

  3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799948 9

  x

  3674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7

# Παραγοντοποιηση

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

# «Πυλώνες» 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

# Σημασία πολυωνυμικού 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!*

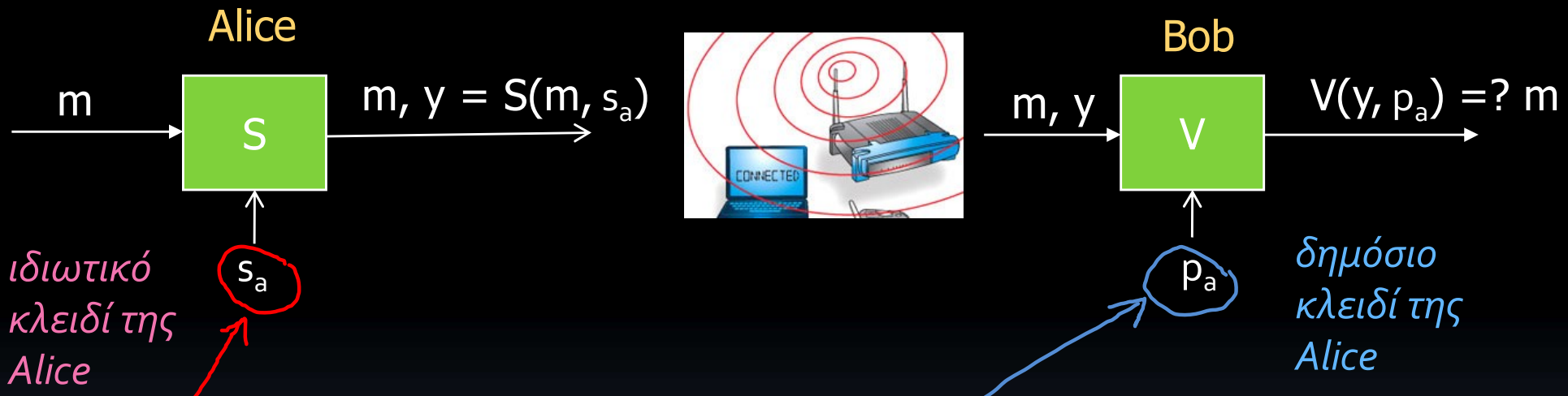
# Ιδιωτικότητα στην πράξη

- 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

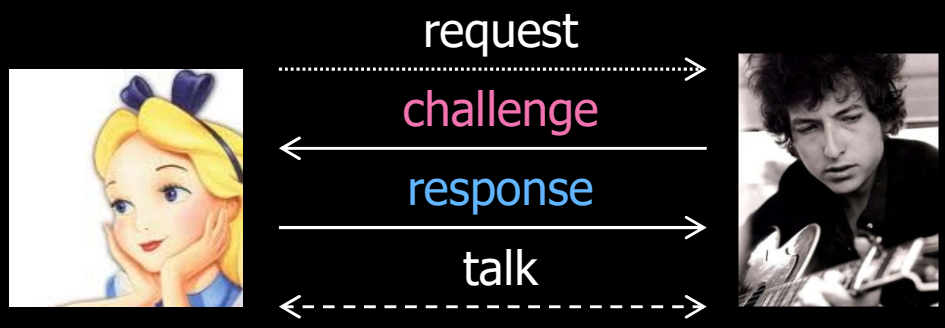
Επαλήθευση




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

# Μια πρώτη ματιά: πρωτόκολλα

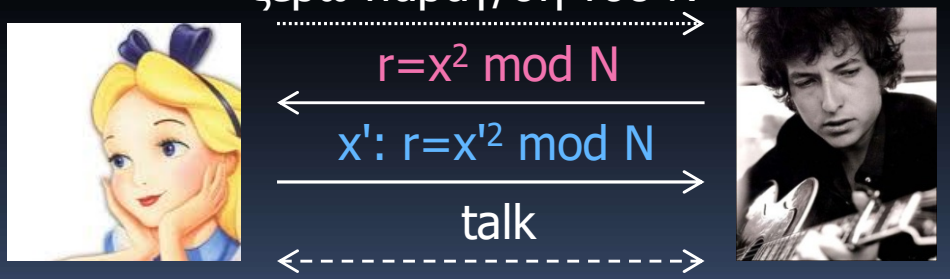
- Ταυτοποίηση / Πιστοποίηση



# Μια πρώτη ματιά: πρωτόκολλα

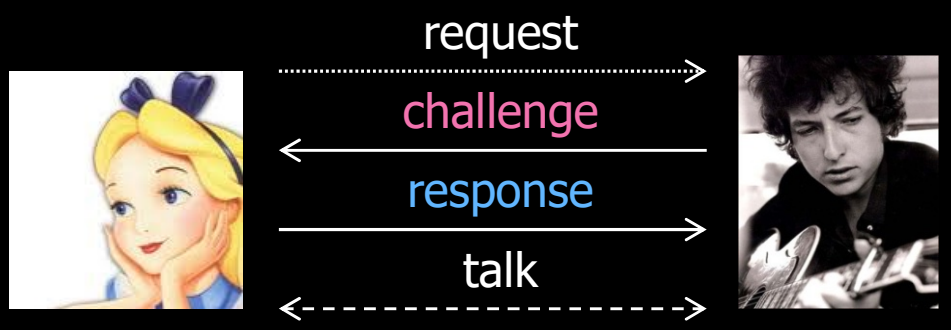
- Ταυτοποίηση / Πιστοποίηση


- Αποδείξεις γνώσης

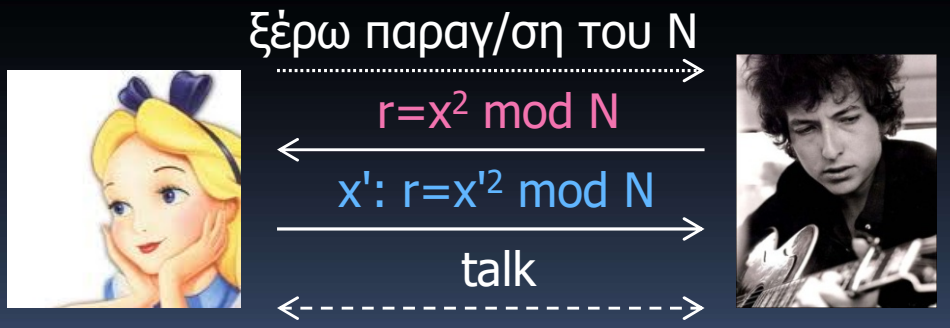


# Μια πρώτη ματιά: πρωτόκολλα

- Ταυτοποίηση / Πιστοποίηση



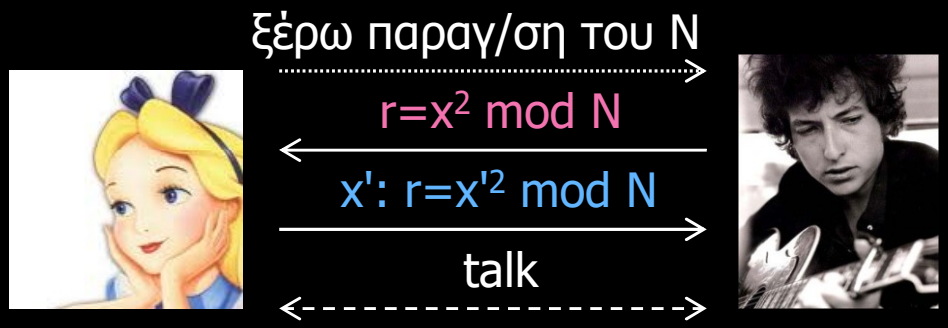

- Αποδείξεις γνώσης




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

# Μια πρώτη ματιά: πρωτόκολλα

- Μη συνειδητή μεταφορά (oblivious transfer)



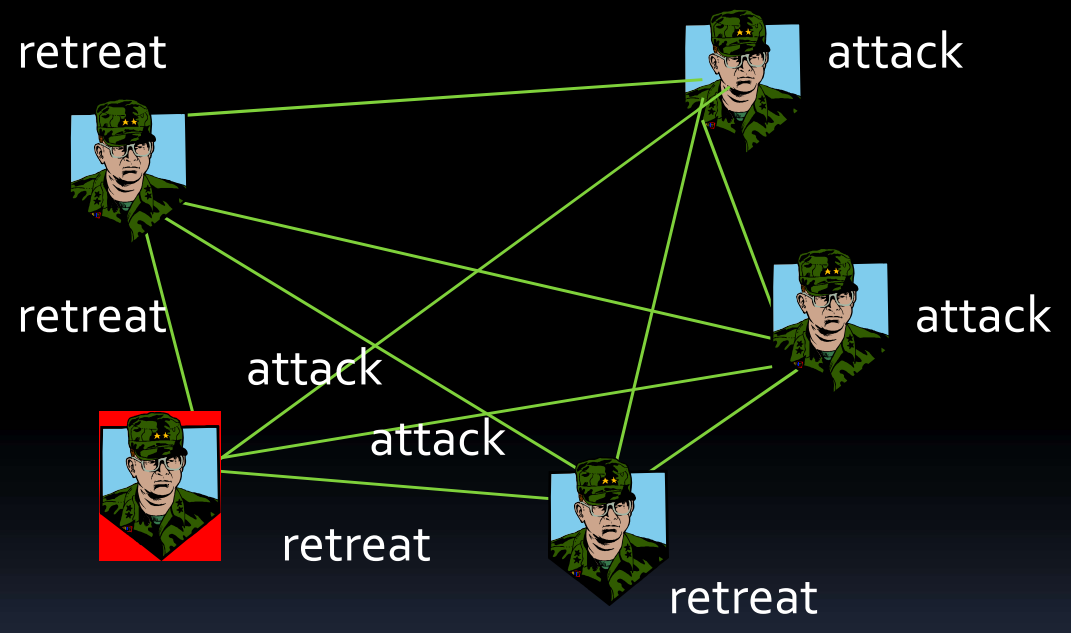

- Η Αλίκη δεν ξέρει αν ο Bob έμαθε κάτι ή όχι
- *Πολύ σημαντικό πρωτόκολλο!*

# Μια πρώτη ματιά: πρωτόκολλα

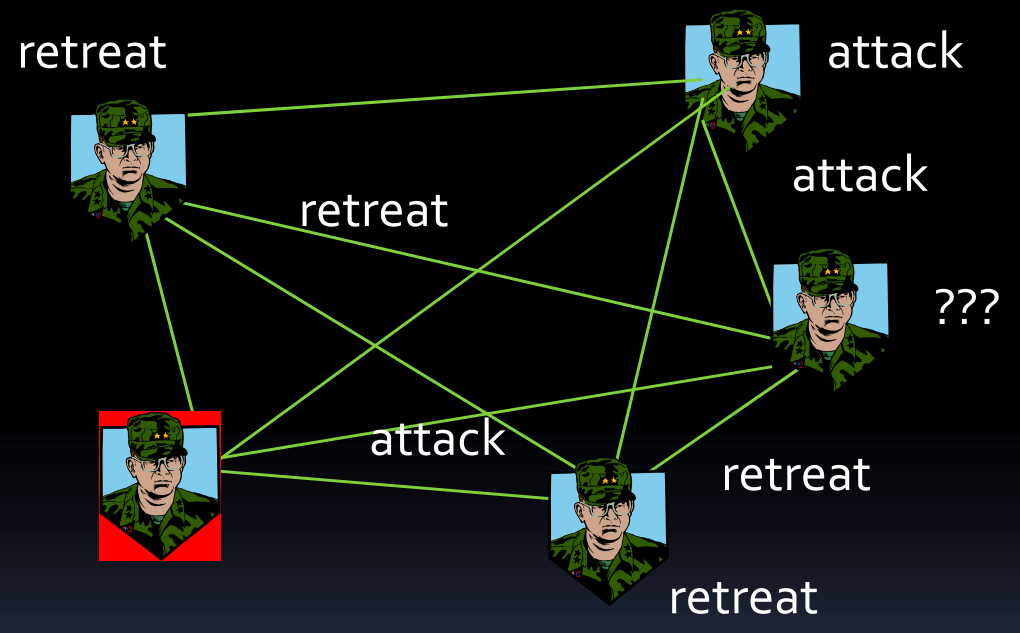
- Tor: ανώνυμη περιήγηση στο δίκτυο

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

# Μια πρώτη ματιά: Byzantine Generals / Consensus

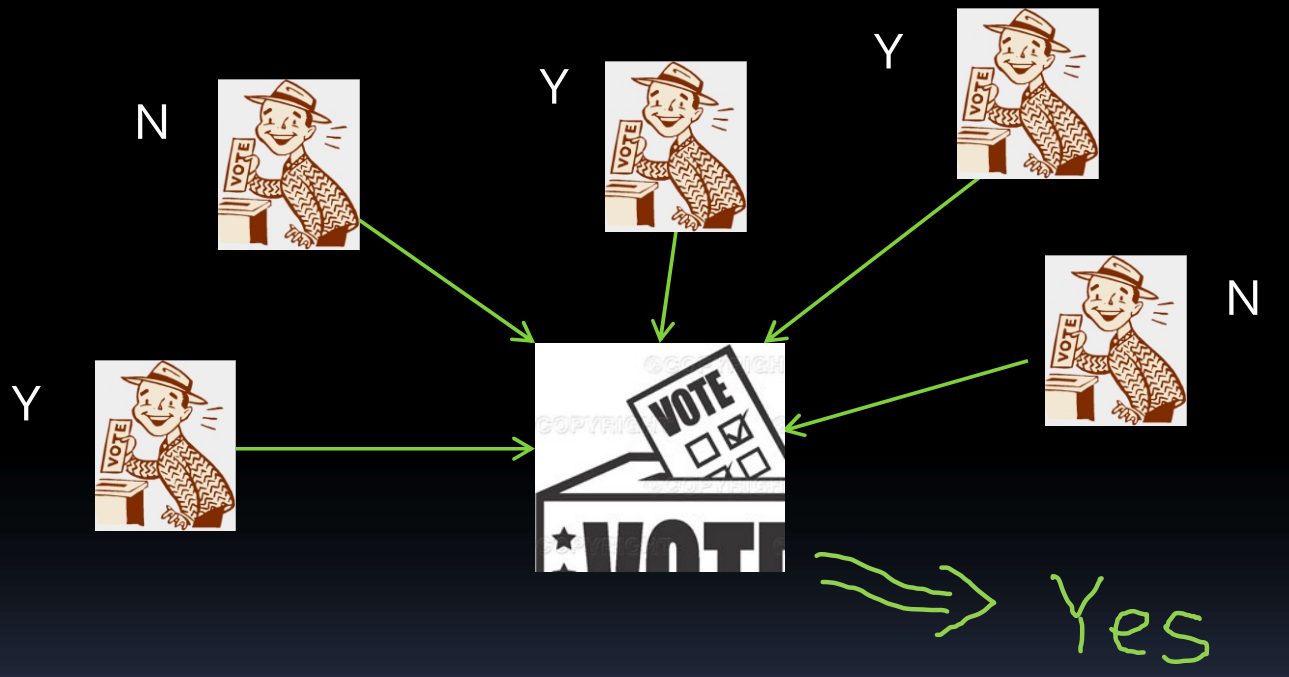


# Μια πρώτη ματιά: Byzantine Generals / Consensus



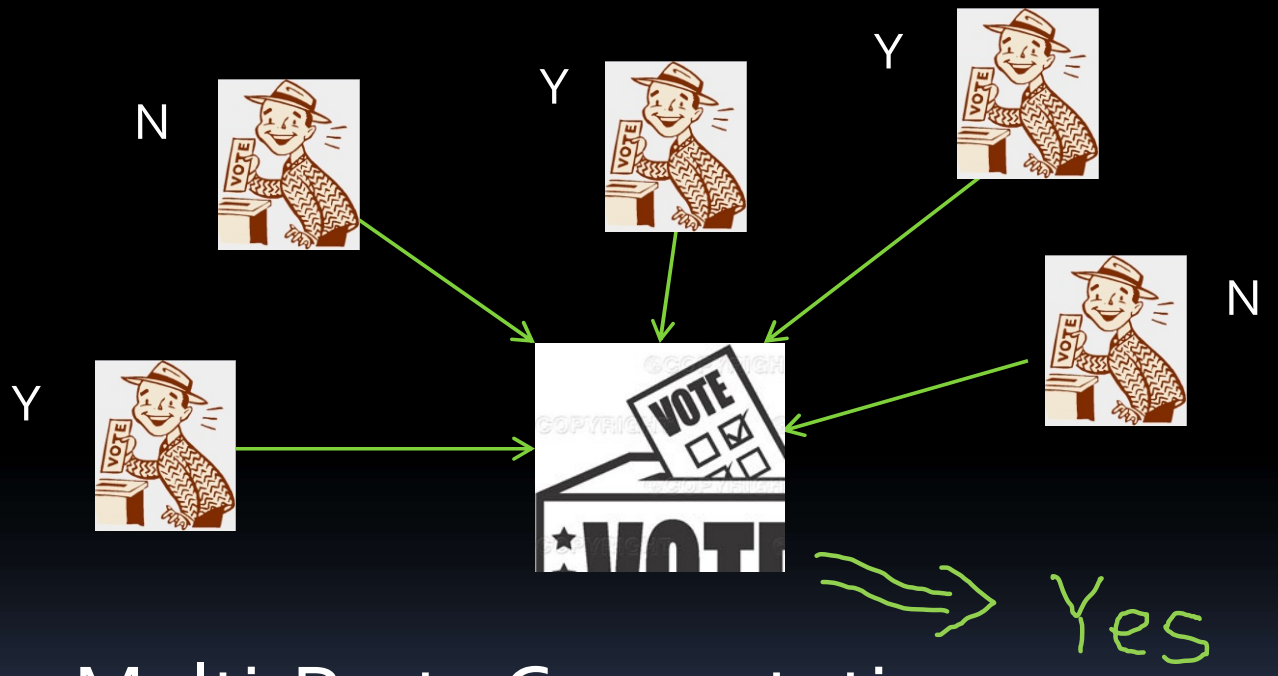
# Μια πρώτη ματιά: e-voting

- Ηλεκτρονικές ψηφοφορίες



# Μια πρώτη ματιά: e-voting

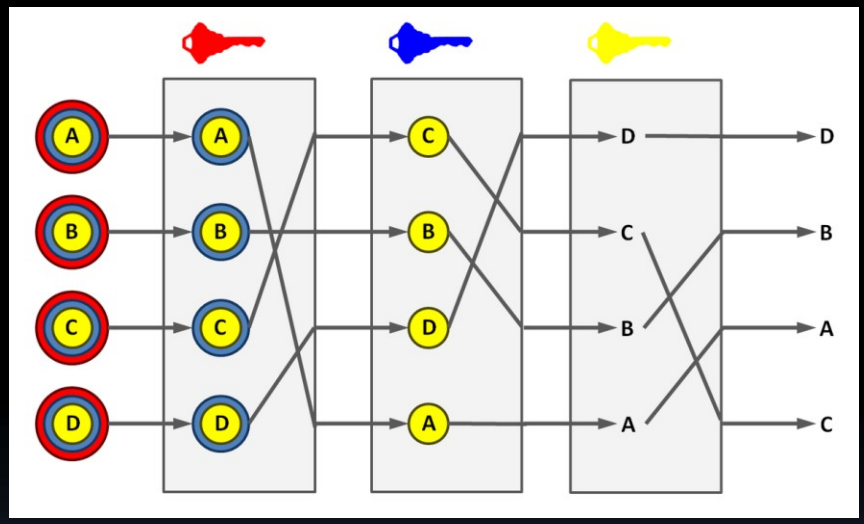
- Ηλεκτρονικές ψηφοφορίες




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

# Μια πρώτη ματιά: ανωνυμία

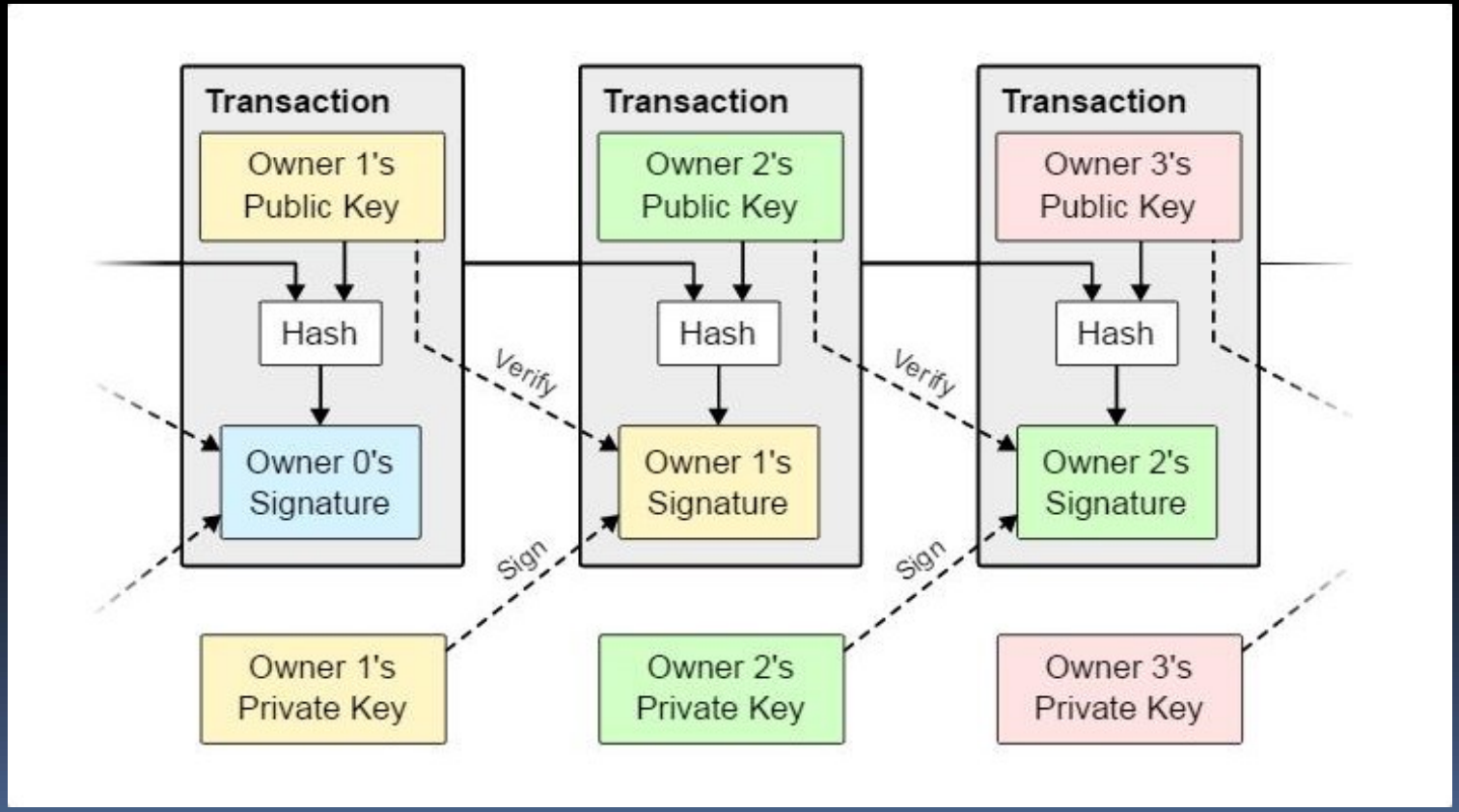
- Τεχνικές ανωνυμοποίησης
  - Mixnets




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

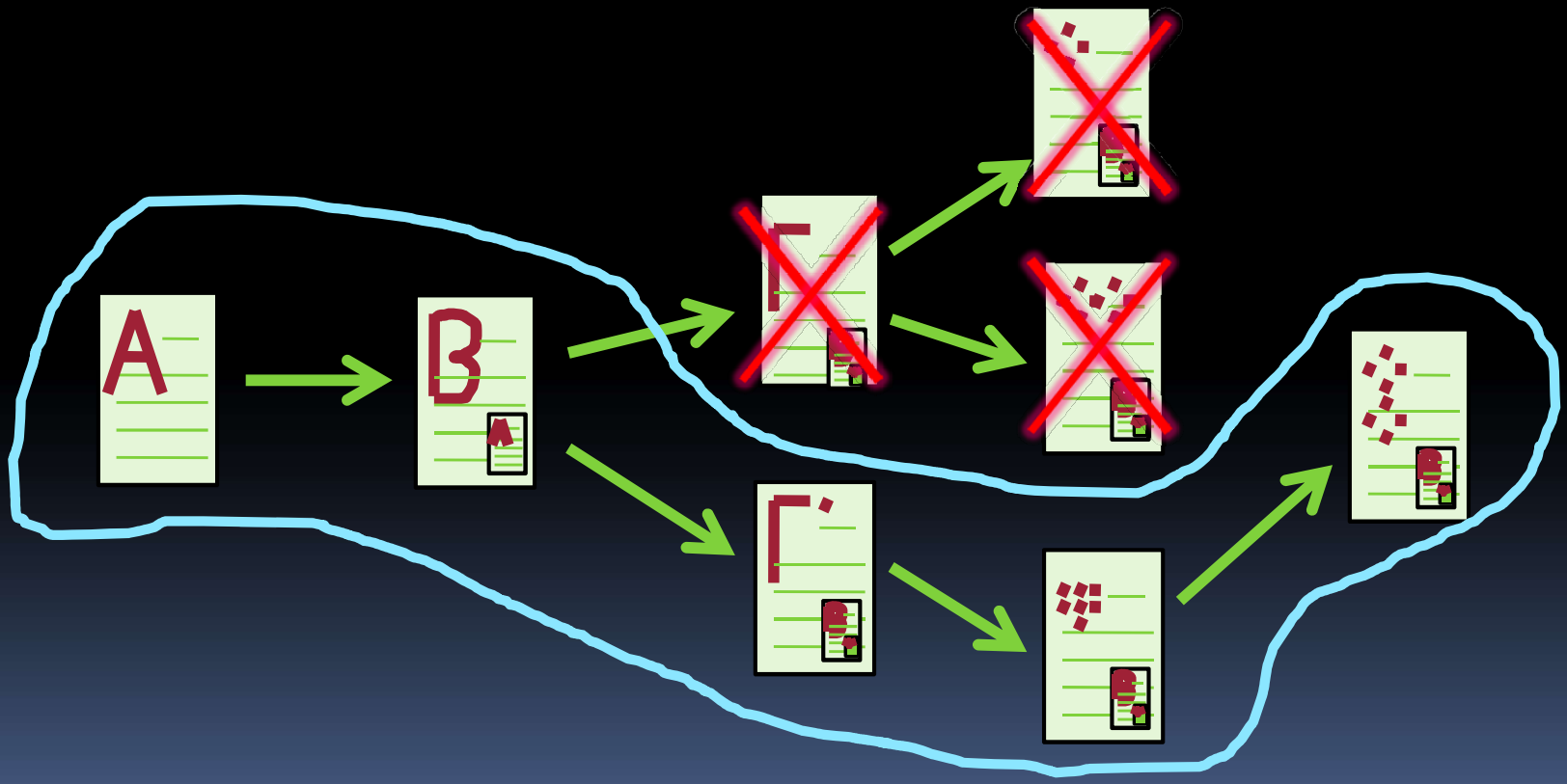
# Μια πρώτη ματιά: blockchain

- Bitcoin [Satoshi Nakamoto 2008]



# Μια πρώτη ματιά: blockchain

- Proof-of-Work (PoW)



# 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 παραπέρα έρευνα!*