ΥΠΟΛΟΓΙΣΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Εισαγωγή

Άρης Παγουρτζής – Στάθης Ζάχος
Σχολή ΗΜΜΥ ΕΜΠ

Διοικητικά του μαθήματος (2016-17)

- Διδάσκοντες
  - Στάθης Ζάχος
  - Άρης Παγουρτζής
  - Πέτρος Ποτίκας
- Βοηθοί διδασκαλίας
  - Παναγιώτης Γροντάς
  - Αντώνης Αντωνόπουλος
  - Γιάννης Παπαϊωάννου
- Βοηθοί ασκήσεων
  - Αντώνης Αγγελάκης
  - Αλέξανδρος Ζαχαράκης
  - Βασίλης Λίβανος
  - Εύα Σαραφιανού

Διοικητικά του μαθήματος (2016-17)

- 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, ...

Σημασία της Κρυπτογραφίας

- Ασφάλεια επικοινωνιών (στρατιωτικών και μη)
- Ασφάλεια / διευκόλυνση συναλλαγών
- Νομικές εφαρμογές (ψηφιακά συμβόλαια)
- 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!

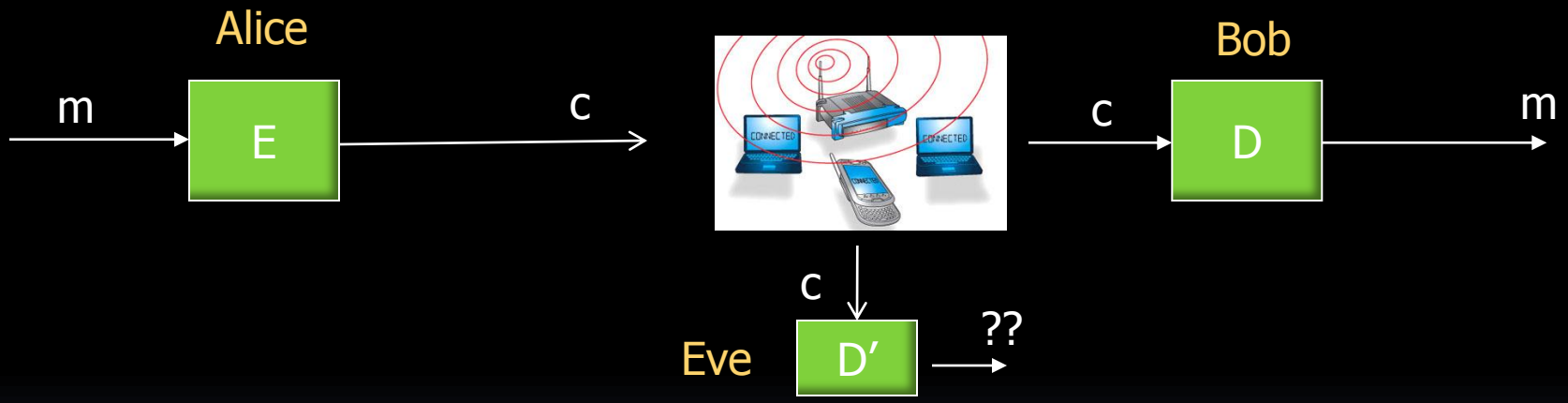
Μια πρώτη ματιά: ιδιωτικότητα

Κρυπτογράφηση

Αποκρυπτογράφηση

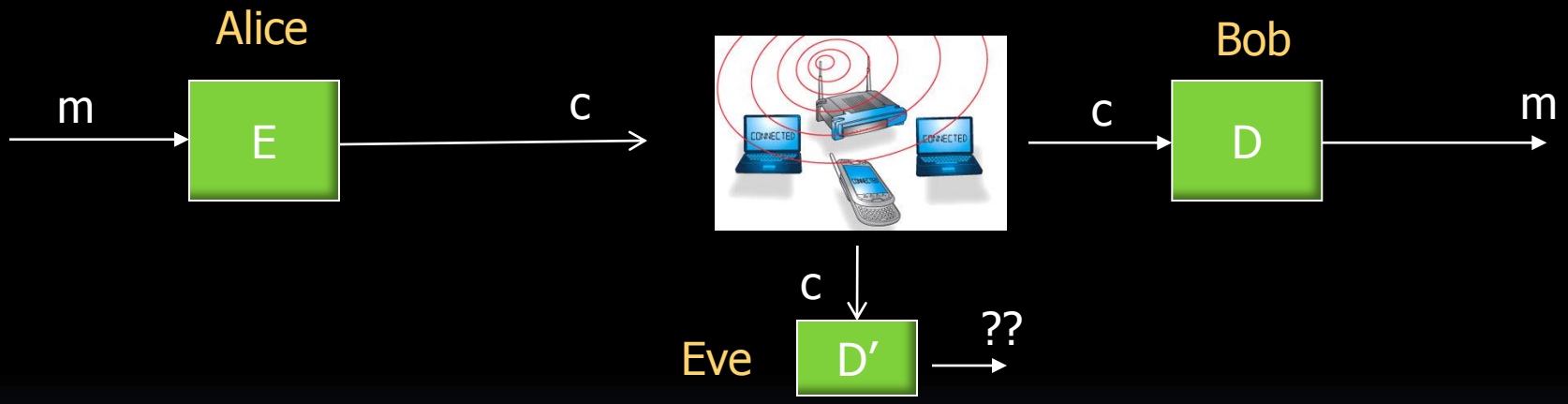
Μια πρώτη ματιά: ιδιωτικότητα

Κρυπτογράφηση Αποκρυπτογράφηση



Μια πρώτη ματιά: ιδιωτικότητα

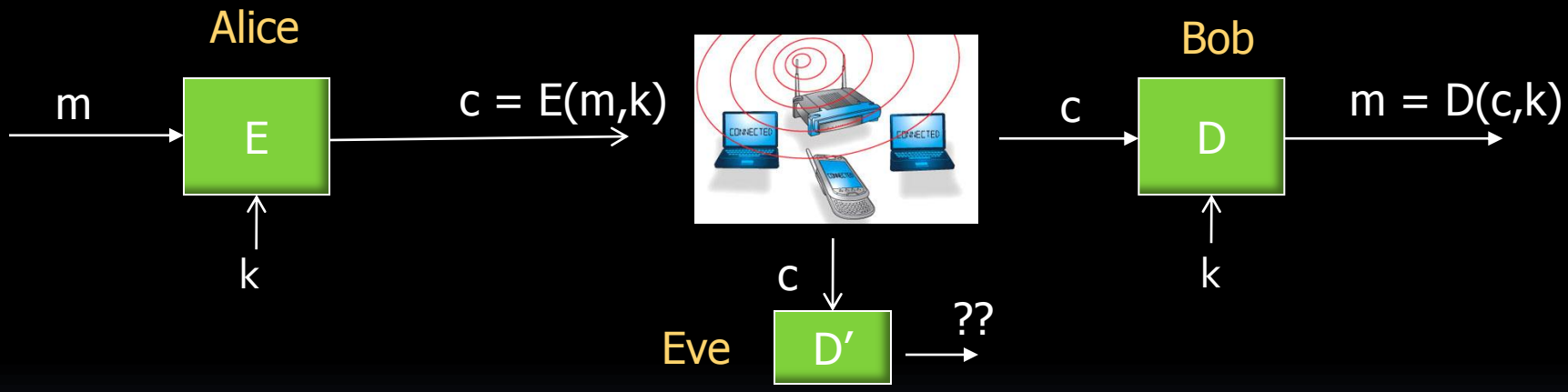
Κρυπτογράφηση Αποκρυπτογράφηση



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

Μια πρώτη ματιά: ιδιωτικότητα

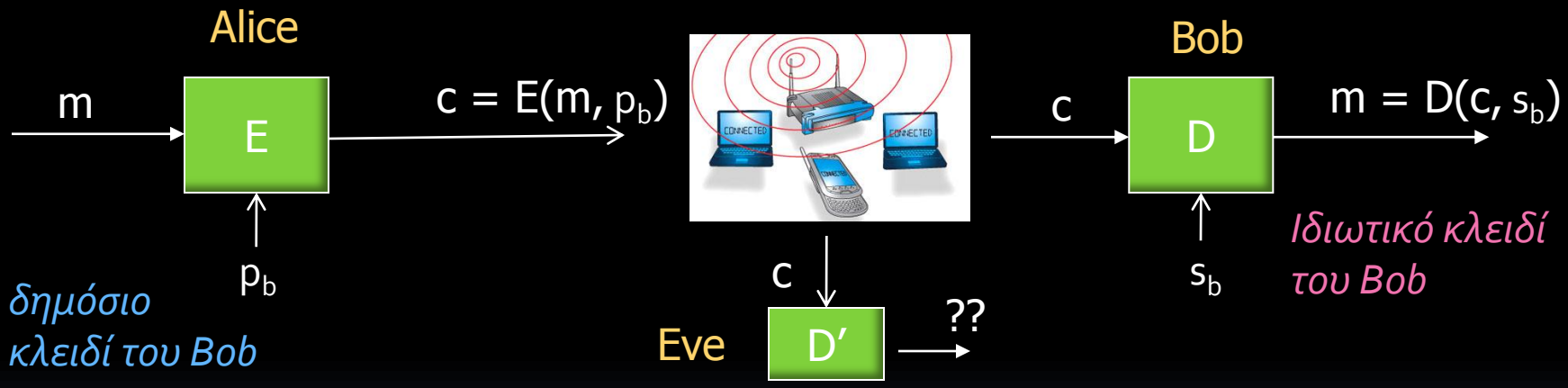
Κρυπτογράφηση Αποκρυπτογράφηση



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

Μια πρώτη ματιά: ιδιωτικότητα

Κρυπτογράφηση Αποκρυπτογράφηση



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

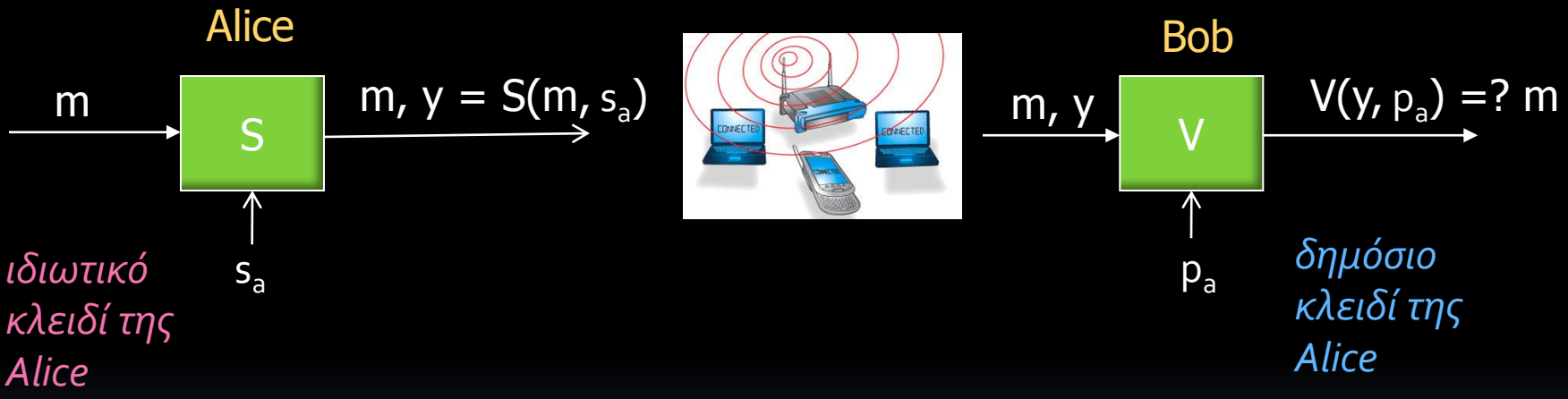
Στην πράξη

- Συνήθης μέθοδος
  - Χρήση πρωτοκόλλων ταυτοποίησης για εγκαθίδρυση επικοινωνίας
  - Χρήση κρυπτογραφίας δημοσίου κλειδιού (π.χ. RSA) 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

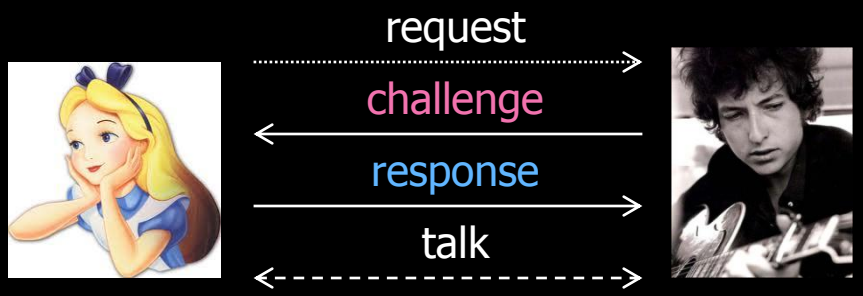
Επαλήθευση



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

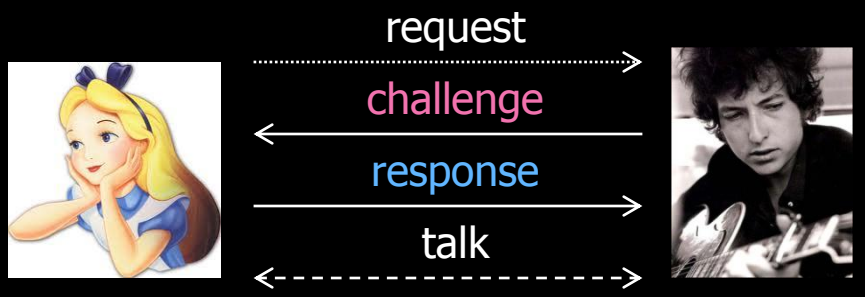
Μια πρώτη ματιά: πρωτόκολλα

- Ταυτοποίηση / Πιστοποίηση

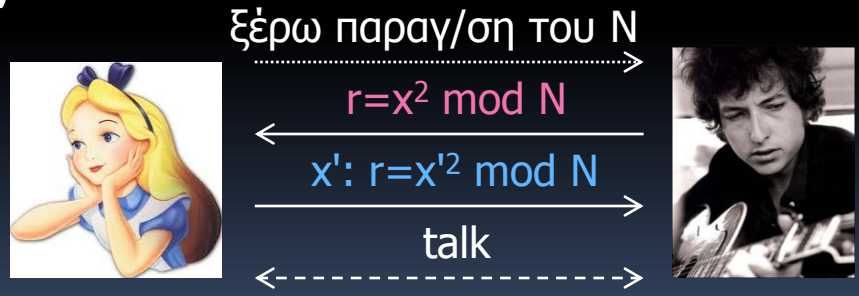


Μια πρώτη ματιά: πρωτόκολλα

- Ταυτοποίηση / Πιστοποίηση

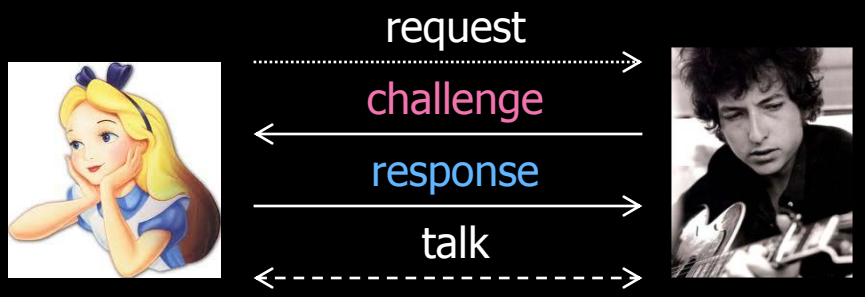


- Αποδείξεις γνώσης

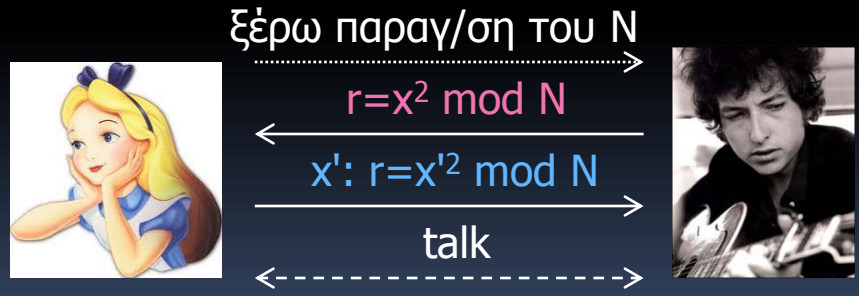


Μια πρώτη ματιά: πρωτόκολλα

- Ταυτοποίηση / Πιστοποίηση



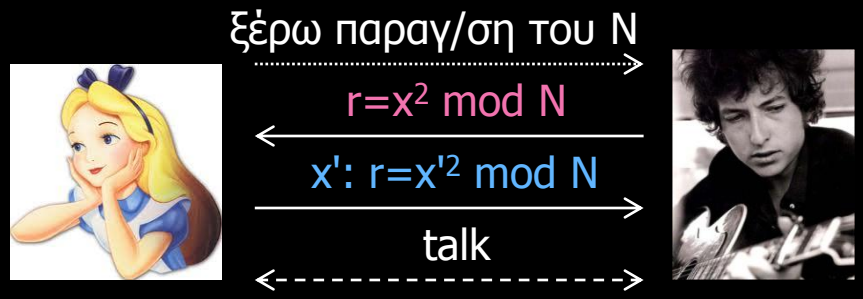
- Αποδείξεις γνώσης



… 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!*

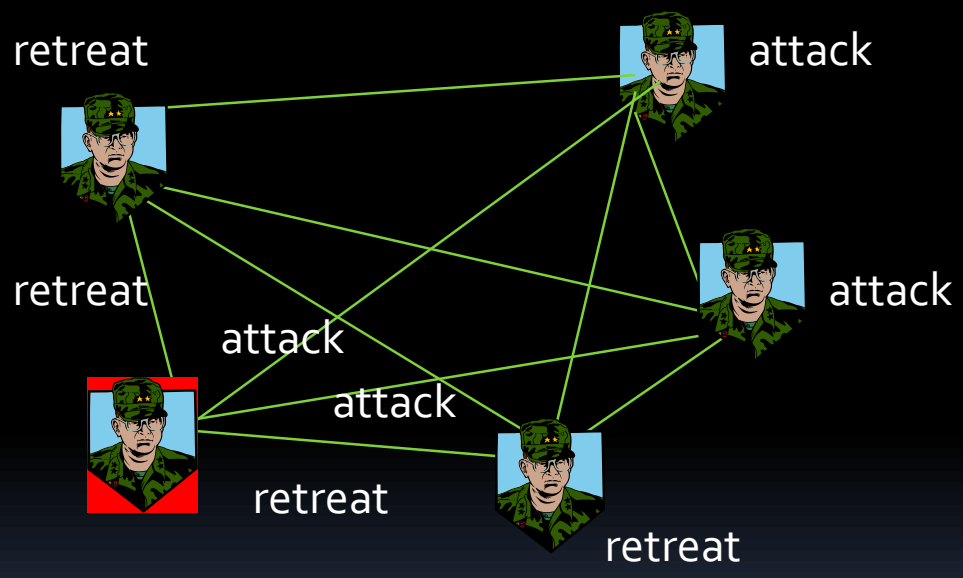
Μια πρώτη ματιά: πρωτόκολλα

- Tor: ανώνυμη περιήγηση στο δίκτυο

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

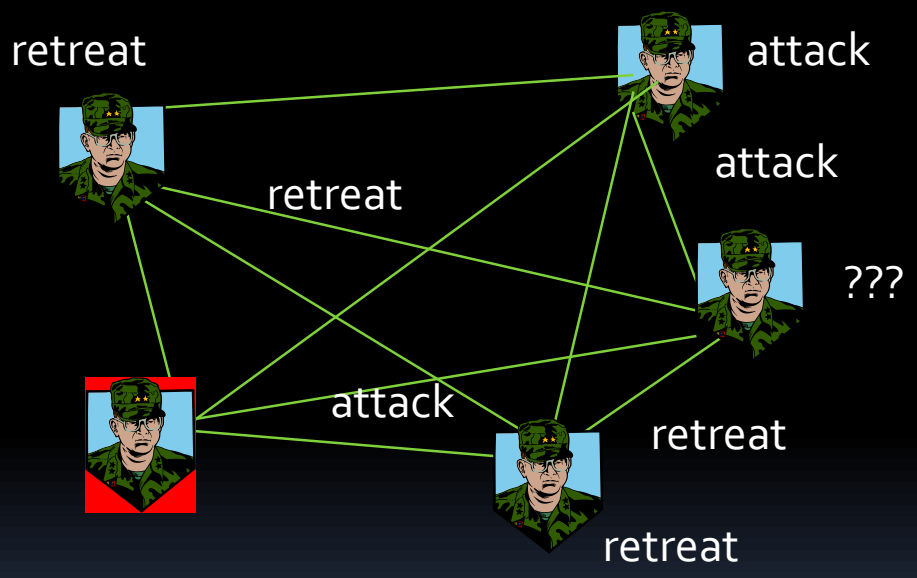
Μια πρώτη ματιά: πρωτόκολλα

- Βυζαντινοί στρατηγοί



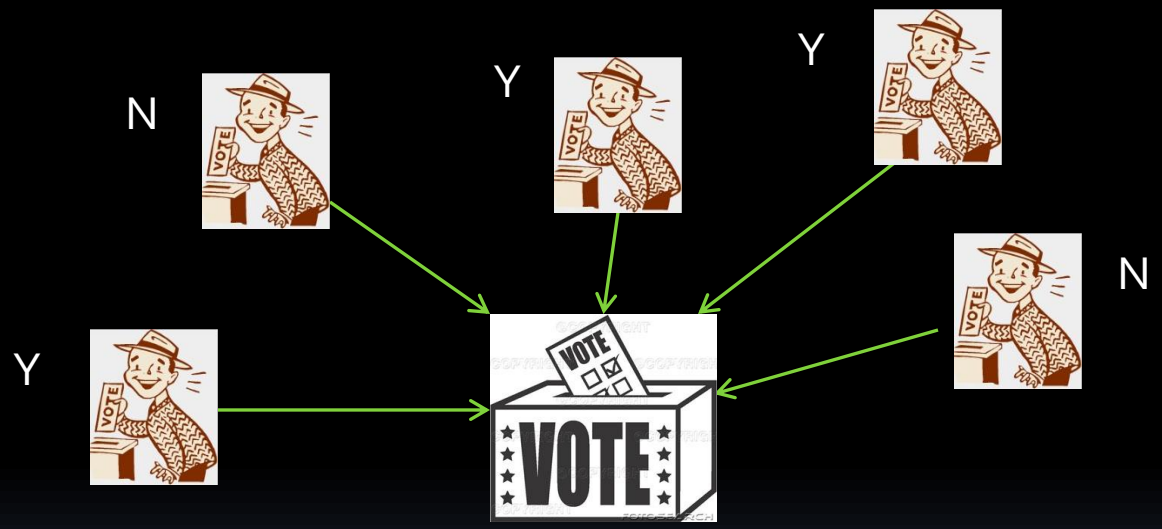
Μια πρώτη ματιά: πρωτόκολλα

- Βυζαντινοί στρατηγοί



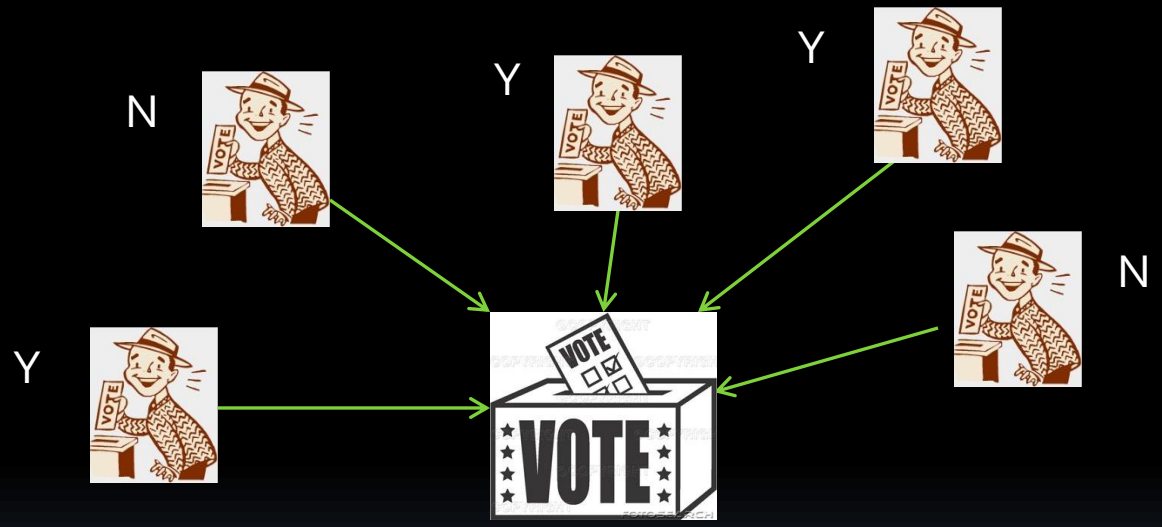
Μια πρώτη ματιά: πρωτόκολλα

- Ηλεκτρονικές ψηφοφορίες



Μια πρώτη ματιά: πρωτόκολλα

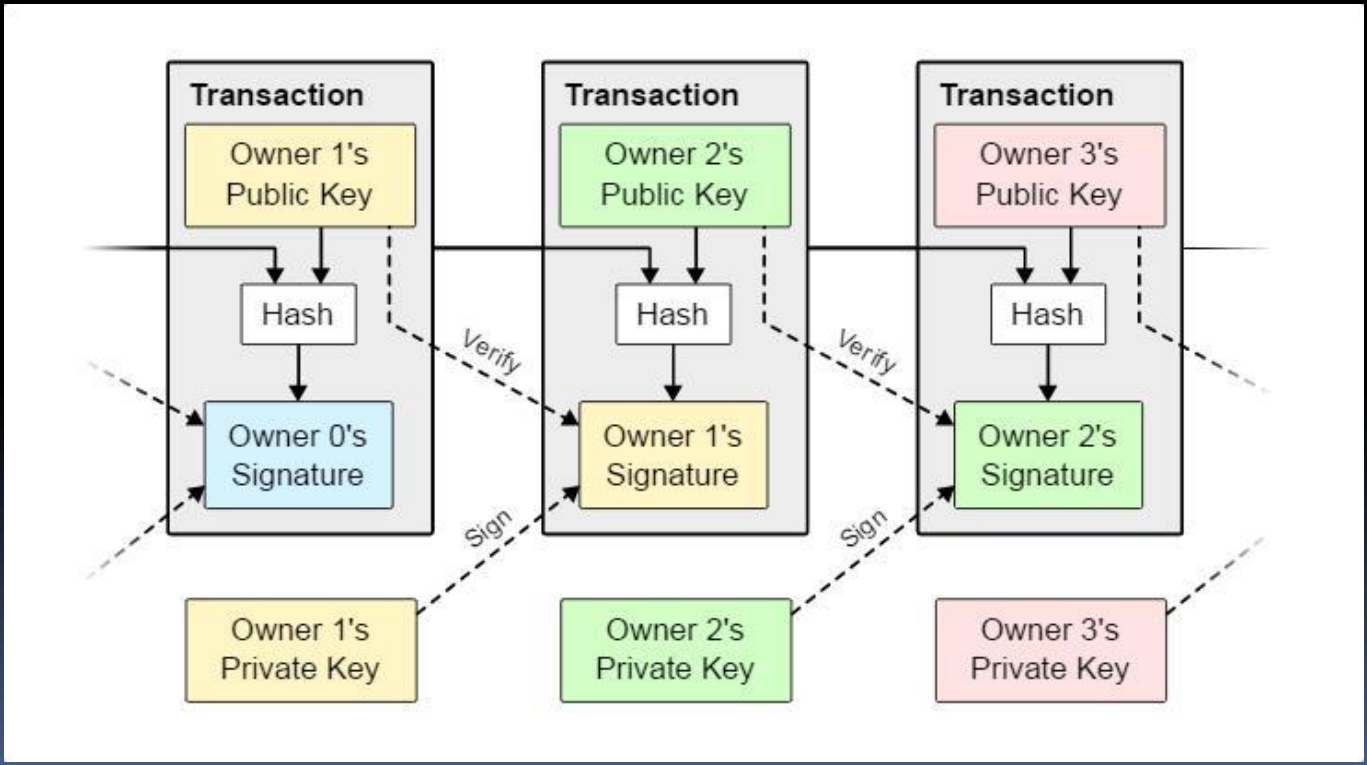
- Ηλεκτρονικές ψηφοφορίες



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

Μια πρώτη ματιά: πρωτόκολλα

- 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!

ΠΑΡΑΡΤΗΜΑ: Το πρόβλημα του 2^{29}

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')