Μια πρόταση διδασκαλίας για την ανταλλαγή κλειδιού Diffie – Hellman (DHKE)

Παναγιώτης Γροντάς

Καλλιτεχνικό Σχολείο Γέρακα

Ιστορικό

Αρχικά ως μέρος της ερευνητικής εργασίας

- 6ο ΓΕΛ Αχαρνών (2011-2012, 2013-2014)
- Με πρωτοβουλία των μαθητών

Μαθήματα επιλογής Α, Β, Γ Λυκείου

- Εφαρμογές υπολογιστών
- Εφαρμογές πληροφορικής (ΚΕΦ.10)

Σε μικρή μερίδα μαθητών Γ Γυμνασίου

Απαιτούμενος Χρόνος:

- 2-3 διδακτικές ώρες

Κίνητρο

Η ανάγκη αναδιάρθρωσης και αναβάθμισης των προγραμμάτων σπουδών

Το παράδοξο της Πληροφορικής στην εκπαίδευση

Πληροφορική ≠ Προγραμματισμός

Πρέπει να δωθεί βάρος σε **θεμελιώδη** προβλήματα

- ... με επιστημονικό βάθος
- ... με σημασία στην καθημερινή ζωή
- ... τα οποία είναι προσβάσιμα στους μαθητές

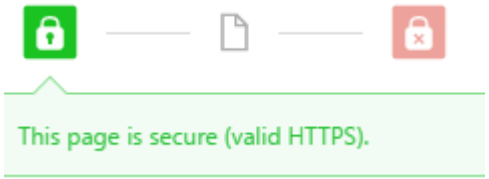
Ναι, υπάρχουν τέτοια προβλήματα

Και υπάρχει και πολύ υλικό ήδη διαθέσιμο

Γιατί DHKE;

Ενσωματωμένη σε συστήματα που χρησιμοποιούνται καθημερινά (SSL/TLS)
- Άρα **χρήσιμο**: εξηγεί ένα «φαινόμενο»
- Δεν είναι **τεχνική γνώση**

Θεμελιώδης Επιστημονική Γνώση
- Επίλυση προβλήματος 2500 ετών
- Κρυπτογραφία Δημοσίου Κλειδιού
- Βραβείο Turing 2015



Απλό στην ουσία του
- Ιδιότητες δυνάμεων (εις διπλούν)
- ... διαθέσιμες και επιπλέον απλοποιήσεις

Εντυπωσιακό
- Επιτυγχάνει που φαίνεται αδύνατο

Γιατί DHKE; (2)

Ως μέρος μιας ευρύτερης εισαγωγής της κρυπτογραφίας στα προγράμματα σπουδών

- Παλαιότερες προτάσεις για συμμετρική κρυπτογραφία
- Εισαγωγή στη Κρυπτογραφία Δημοσίου Κλειδιού

Γιατί Κρυπτογραφία;

- Άμεση σχέση με θεμελιώδη προβλήματα της Πληροφορικής
- Διαθεματικότητα:
  - Μαθηματικά
  - Ιστορία
  - Ατομικές ελευθερίες στον σύγχρονο κόσμο
  - Εμπιστοσύνη πέρα από Μυστικότητα
- Ενδιαφέρει πολύ τους μαθητές!
  - Πρέπει να διδαχθεί υπεύθυνα και ισορροπημένα

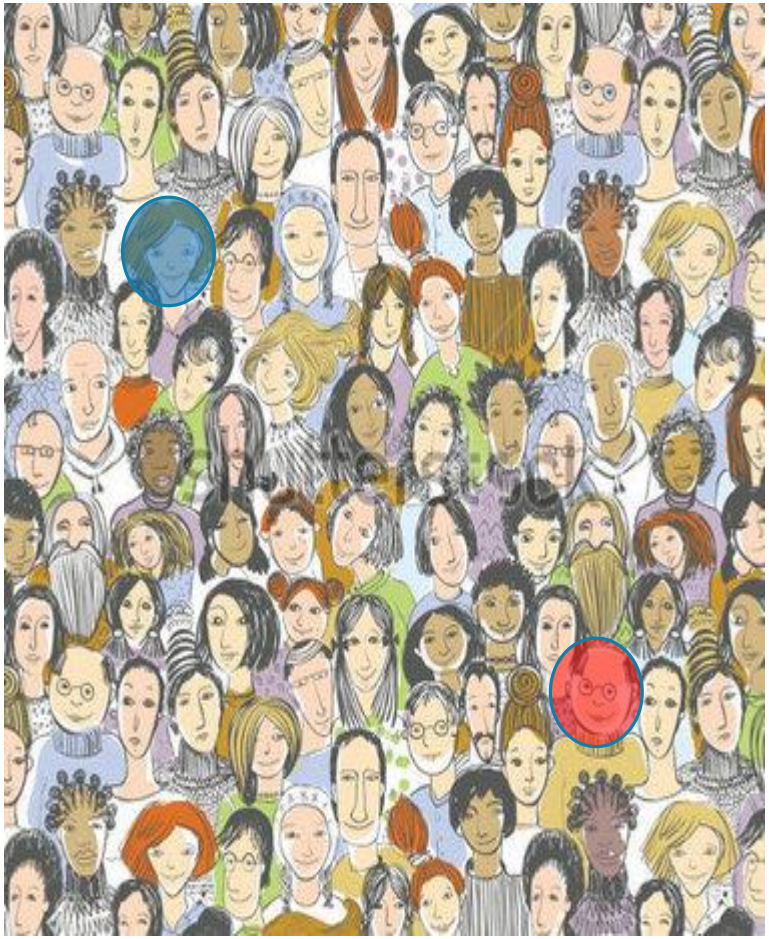
Δημιουργία γενικού πλαισίου

Αποσαφήνιση εννοιών / μεθόδων κρυπτογραφίας

- Επίκληση γνώσων μαθητών:
  - Συμμετρική κρυπτογραφία
- Ιστορικά παραδείγματα:
  - Σπαρτιατική σκυτάλη
  - Κρυπτογράφημα Καίσαρα
  - Μηχανή Enigma
- Στόχος: να τονίσουμε:
  - τη σημασία και η μορφή του κλειδιού
  - την εκ των προτέρων συμφωνία κλειδιού στα συμμετρικά συστήματα
- Ερώτημα: Μπορεί να γίνει κάτι αντίστοιχο στο Διαδίκτυο;
- Γιατί όχι;

Πετυχαίνοντας το αδύνατο (με αναλογίες)

- Μυστική επικοινωνία σε ένα δωμάτιο γεμάτο κόσμο (ωτακουστές)
- Πρέπει μέσω μιας συζήτησης που παρακολουθούν και καταλαβαίνουν όλοι
- να δημιουργηθεί **επιτόπου μία ξένη γλώσσα**
- που να μην καταλαβαίνει κανένας άλλους
- **Πρόκληση προς τους μαθητές, με επισήμανση της δυσκολίας**



Η λύση (DH76): Ιδιότητες δυνάμεων

2. Επιλογή μυστικού εκθέτη α

1.Επιλογή βάσης γ

3. γ^{α}

3. γ^{β}

2. Επιλογή μυστικού εκθέτη β

4. $k = (\gamma^{\beta})^{\alpha} = \gamma^{\alpha\beta}$

4. $k = (\gamma^{\alpha})^{\beta} = \gamma^{\alpha\beta}$

«Άχρηστες Λεπτομέρειες»: *γ γεννήτορας κυκλικής ομαδας τάξης q, α,β ∈ Zq*

«Απλά λέμε»: *γ, α,β* ***ειδικοί*** *μεγάλοι αριθμοί*

Γενικευμένο μοντέλο πρωτοκόλλου

Δημόσια συμφωνία βάσης
- Μπορεί να επιλεγούν αυθαίρετα

Επιλογή μυστικών πληροφοριών

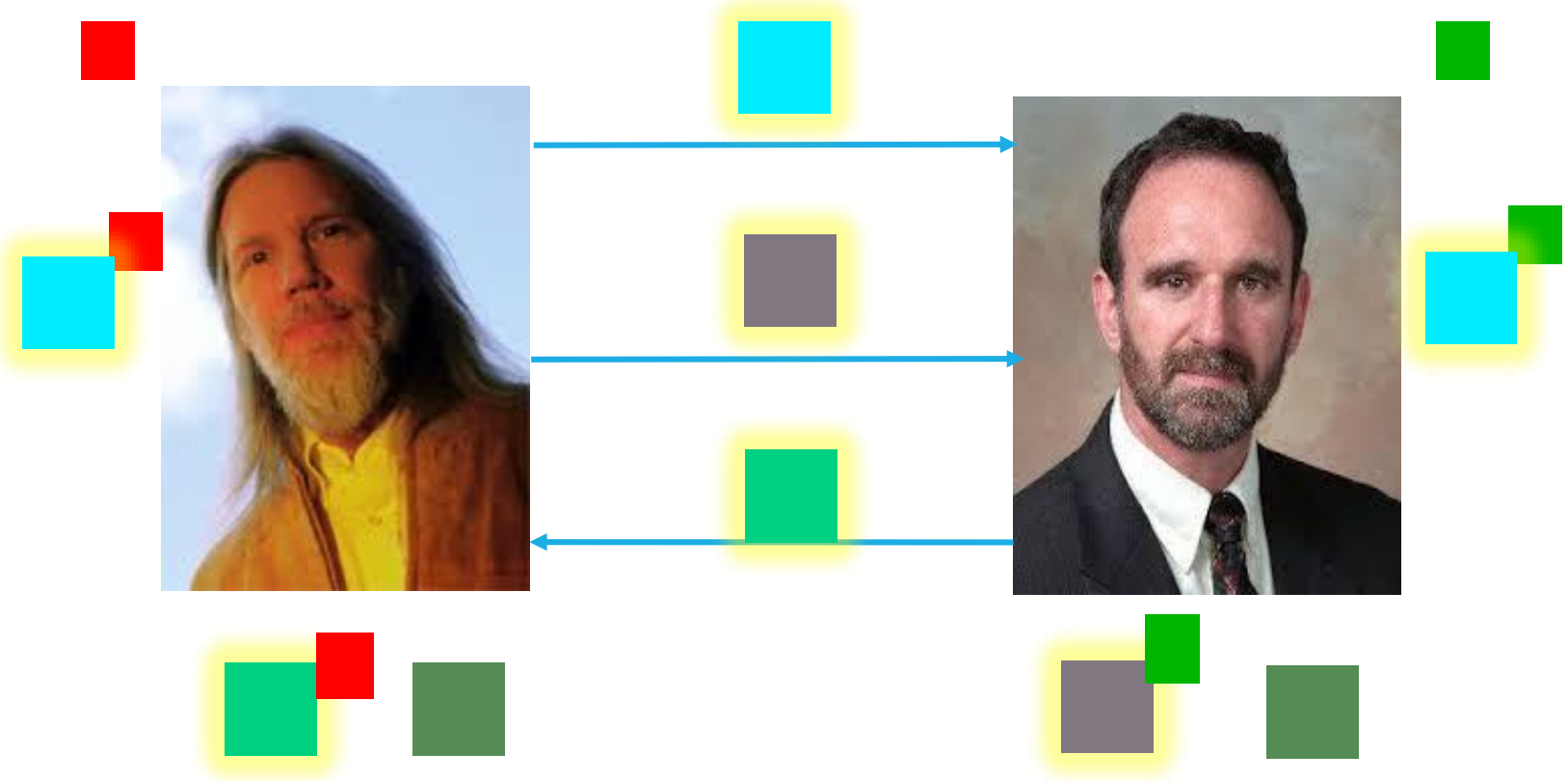
(teacher only)

(Ιδιωτική) Μίξη παραμέτρων 1 και μυστικού 2 και ανταλλαγή

(Ιδιωτική) Μίξη μυστικού 2 και μηνύματος 3

Επιλογή διδακτικών προσεγγίσεων για τη μίξη
- Κατανόηση
- Ασφάλεια

Μίξη με χρώματα (Singh -2001, Kahn Academy)



http://trycolors.com/

Συζήτηση για την ασφάλεια

Καταιγισμός Ιδεών (με καθοδήγηση):

- Τι πρέπει να προστατευθεί
- Επισήμανση διαχωρισμού δημοσίων από ιδιωτικά χρώματα
  - Πιθανές απαντήσεις:
    - Ιδιωτικά Χρώματα
    - Κοινό Χρώμα
- Τρόποι Επίθεσης:
  - Ανάκτηση Κοινού Χρώματος
    - Μέσω των ιδιωτικών χρωμάτων
    - Μόνο από τα δημόσια χρωμάτα
- Κατάταξη ως προς δυσκολία

Συζήτηση για την ασφάλεια (2)

Με ορολογία δυνάμεων

Επίθεση 1: Χωρίς τα ιδιωτικά κλειδιά (CDHP)
- Υπολογισμός του $\gamma^{\alpha\beta}$ άπό τα γ^{a}, γ^{β}

Επίθεση 2: Διακριτός λογάριθμος (DLP)
- Εύρεση α από γ^{a}
- Εύρεση β από γ^{β}
- Υπολογισμός $\gamma^{\alpha\beta}$

Κατάταξη ως προς τη δυσκολία (αναγωγή)
- Ποιο από τα 2 προβλήματα λύνεται άμεσα αν λυθεί το άλλο; (CDHP ≤ DLP)

Αν υπάρχει χρόνος … πρόκληση για:
- Άλλες επιθέσεις (MITM)

Δυσκολίες

Το όνομα μπερδεύει

- Δημιουργία όχι ανταλλαγή κλειδιού

Τι γίνεται μετά την ανταλλαγή;

- Η σημασία της προτετοιμασίας
- Συζήτηση για το ρόλο του κλειδιού

Σύγκρουση με προηγούμενες αναπαραστάσεις

- Μήνυμα: Ο συμβολισμός για τη δύναμη (γ^{α}) μπερδεύει:
  - Προδιαγραφή πράξης: υπολογισμός δύναμης
  - Αποτέλεσμα πράξης: ένας αριθμός
  - Δημόσια πληροφορία: γ, αποτέλεσμα
  - Ιδιωτική πληροφορία: α
  - Εδώ βοηθούν τα χρώματα και αριθμητικά παραδείγματα

Δυσκολίες (2)

- Αδυναμία αποδοχής δυσκολίας διακριτού λογαρίθμου
  - Σύγχυση με συμβολισμό log (πάλι)
  - Μία συνηθισμένη συμβολική πράξη στην Β και Γ Λυκείου
    - *Επειδή μπορώ να το συμβολίσω δε σημαίνει ότι μπορώ και να το υπολογίσω (εύκολα)*
  - Διαφορά πραγματικών με ακέραιους
  - Για μεγάλους **κατάλληλους** ακέραιους λύση μόνο με εξαντλητικές δοκιμές

(Επιπλέον) Ωφέλη

Καλύτερη κατανόηση της έννοιας του υπολογισμού και διάκριση από την αναπαράστασή του

- Οι μαθητές νομίζουν ότι οι υπολογισμοί γίνονται αυτόματα
- Το μέγεθος της εισόδου επιδρά στον χρόνο ενός υπολογισμού

Εισαγωγή στον κατανεμημένο υπολογισμό

- Δύο οντότητες δουλεύουν ταυτόχρονα στην επίλυση ενός προβλήματος

(Επιπλέον) Ωφέλη (2)

Εισαγωγή στην ασυμμετρία κάποιων υπολογισμών

- Μία κατεύθυνση εύκολη
- Η άλλη δύσκολη

Εισαγωγή σε έννοιες της υπολογιστικής πολυπλοκότητας

- Δεν έχει νόημα η εξαντλητική δοκιμή λύσεων
- Πρακτικά τα επιλύσιμα προβλήματα γίνονται άλυτα (γ γυμνασίου)
- ... με θετικές και αρνητικές συνέπειες ...

Ερωτήσεις