Κρυπτογραφία
ΠΜΣ Πληροφορική

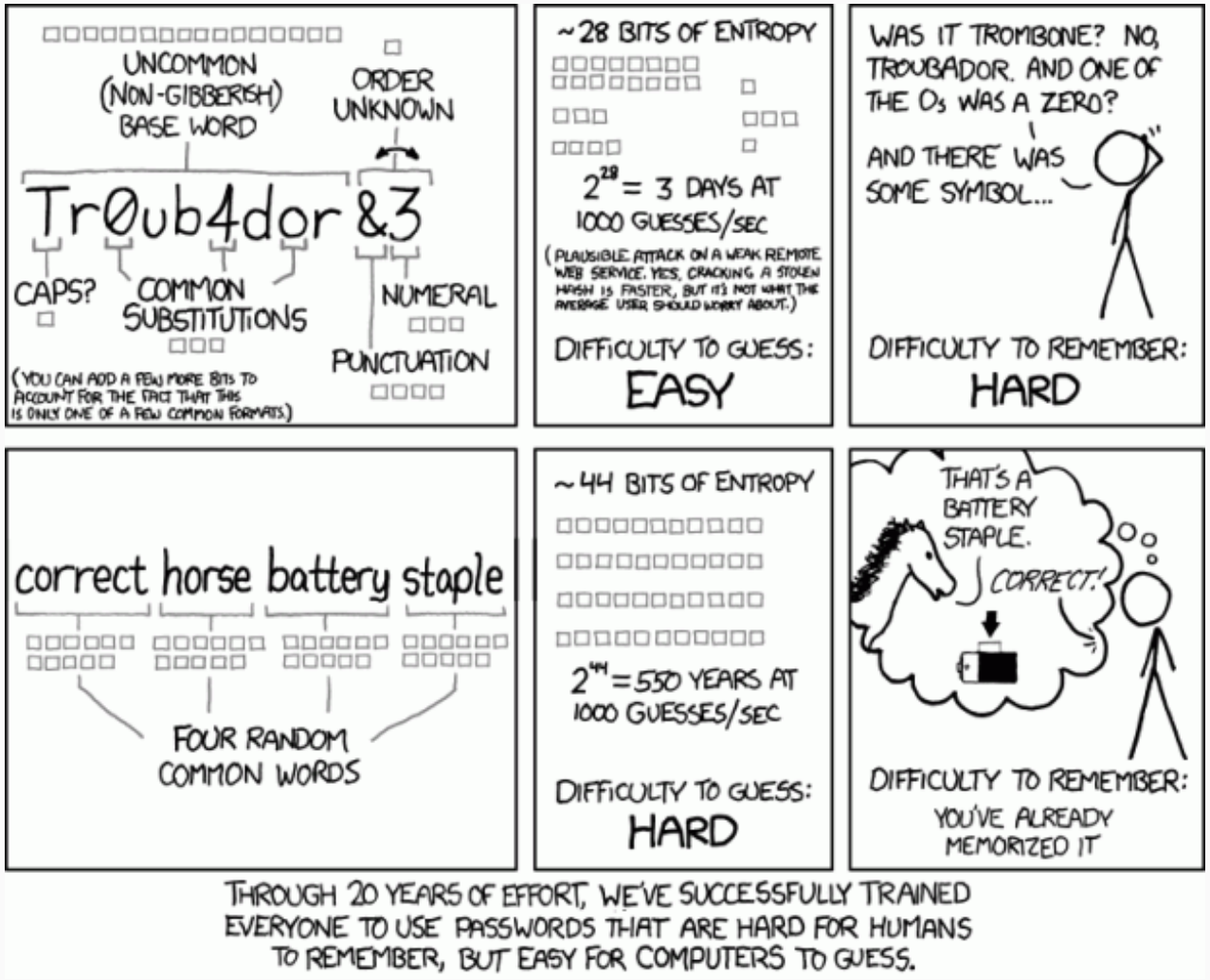
Επ. Καθηγητής Κωνσταντίνος Πατσάκης

October 20, 2017

Τμήμα Πληροφορικής–Πανεπιστήμιο Πειραιώς

Κωδικοί

Σε όλα τα συστήματα προτείνεται η δημιουργία μεγάλων κωδικών πρόσβασης. Δεν αρκεί όμως αυτό.

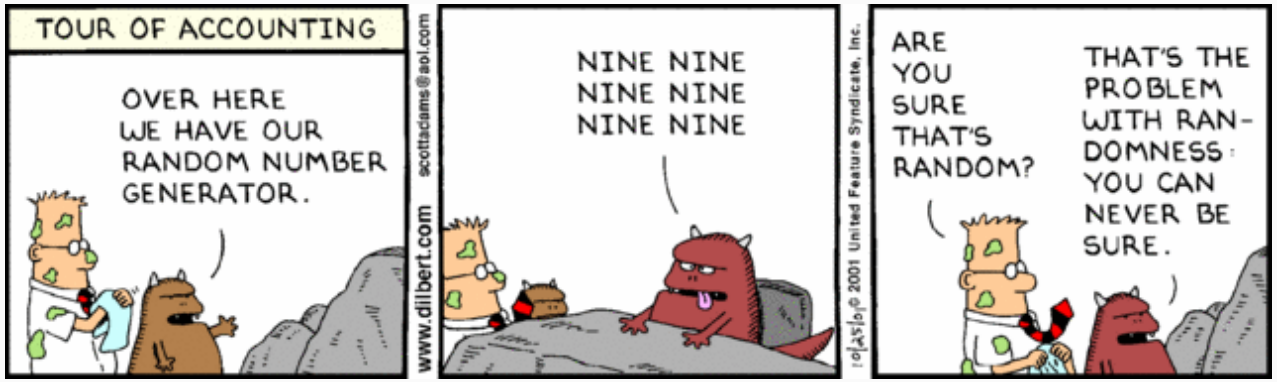


Τυχαιότητα

Πρέπει να έχουμε και τυχαίους κωδικούς

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

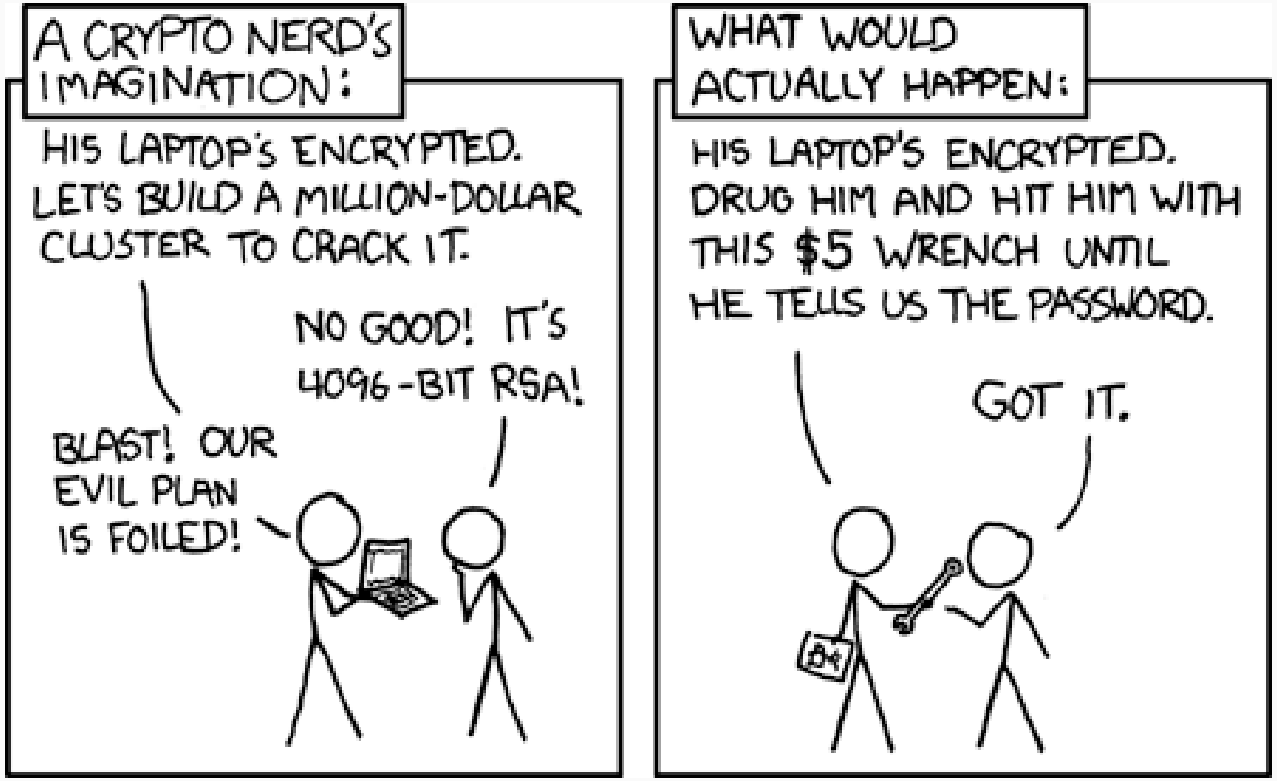
ή τουλάχιστον αυτό το οποίο φαίνεται να μοιάζει τυχαίο.



Τι όμως είναι τυχαίο;

Πραγματική ασφάλεια

Αυτή τη στιγμή έχουμε πολλούς ασφαλείς αλγόριθμους κρυπτογράφησης που δεν μπορούν να ”σπάσουν”, υπάρχουν όμως και άλλες επιθέσεις...



Σκοπός του μαθήματος

1. Αναδρομή από το παρελθόν (Τέχνη) στο σήμερα (Επιστήμη). Αλγόριθμοι που έχουν χρησιμοποιηθεί και γιατί είχαν πρόβλημα.
2. Σύγχρονοι αλγόριθμοι
3. Εφαρμογές

Navajos: Director's cut

Σύγχρονοι αλγόριθμοι

- Αλγόριθμοι ιδιωτικού κλειδιού: DES, RC4, AES,
- Αλγόριθμοι δημοσίου κλειδιού: RSA, ElGamal, Ελλειπτικές καμπύλες
- Συναρτήσεις κατακερματισμού
- Ψηφιακές υπογραφές

Πρωτόκολλα

- Diffie-Hellman
- TLS
- Authentication (PBKDF2, Hash-based authentication, OTP)
- Private Set Intersection (PSI)
- Private Set Similarity (PSI)

PGP

Πως μπορώ να χρησιμοποιήσω τα παραπάνω σε πρακτικές εφαρμογές; Εργαλεία κρυπτογράφησης (openssl, PGP κ.ά.).

Διδασκαλία

7 Διαλέξεις 3 Εργαστήρια (Python/Sage)

Τρόπος εξέτασης: Εργασίες

Επικοινωνία

- Γραφείο: 540 (5ος όροφος)
- Τηλέφωνο: 210 4142261
- email:
  - kpatsak@gmail.com
  - kpatsak@unipi.gr
  - kpatsak@protonmail.ch
- Ιστοσελίδα: `www.cs.unipi.gr/kpatsak`

Ερωτήσεις;