

# Κρυπτογραφία

## ΠΜΣ Πληροφορική

---

Επ. Καθηγητής Κωνσταντίνος Πατσάκης  
October 20, 2017

Τμήμα Πληροφορικής–Πανεπιστήμιο Πειραιώς

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

<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor &amp;3</p> <p>CAPS?      COMMON SUBSTITUTIONS      NUMERAL</p> <p>PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON EXAMPLES.)</p>	<p>~28 BITS OF ENTROPY</p> <p><math>2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STORED HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: <b>EASY</b></p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p> <p>DIFFICULTY TO REMEMBER: <b>HARD</b></p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p><math>2^{44} = 530 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>DIFFICULTY TO GUESS: <b>HARD</b></p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p> <p>DIFFICULTY TO REMEMBER: <b>YOU'VE ALREADY MEMORIZED IT</b></p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Πρέπει να έχουμε και τυχαίους κωδικούς

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

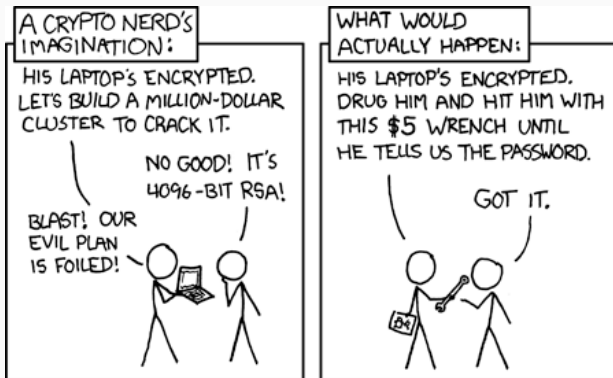
ή τουλάχιστον αυτό το οποίο φαίνεται να μοιάζει τυχαίο.



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



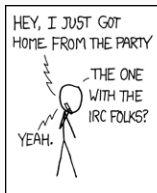
# Σύγχρονοι αλγόριθμοι

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

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



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



7 Διαλέξεις 3 Εργαστήρια (Python/Sage)

Τρόπος εξέτασης: Εργασίες

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

Ευχαριστώ

# Ερωτήσεις;

