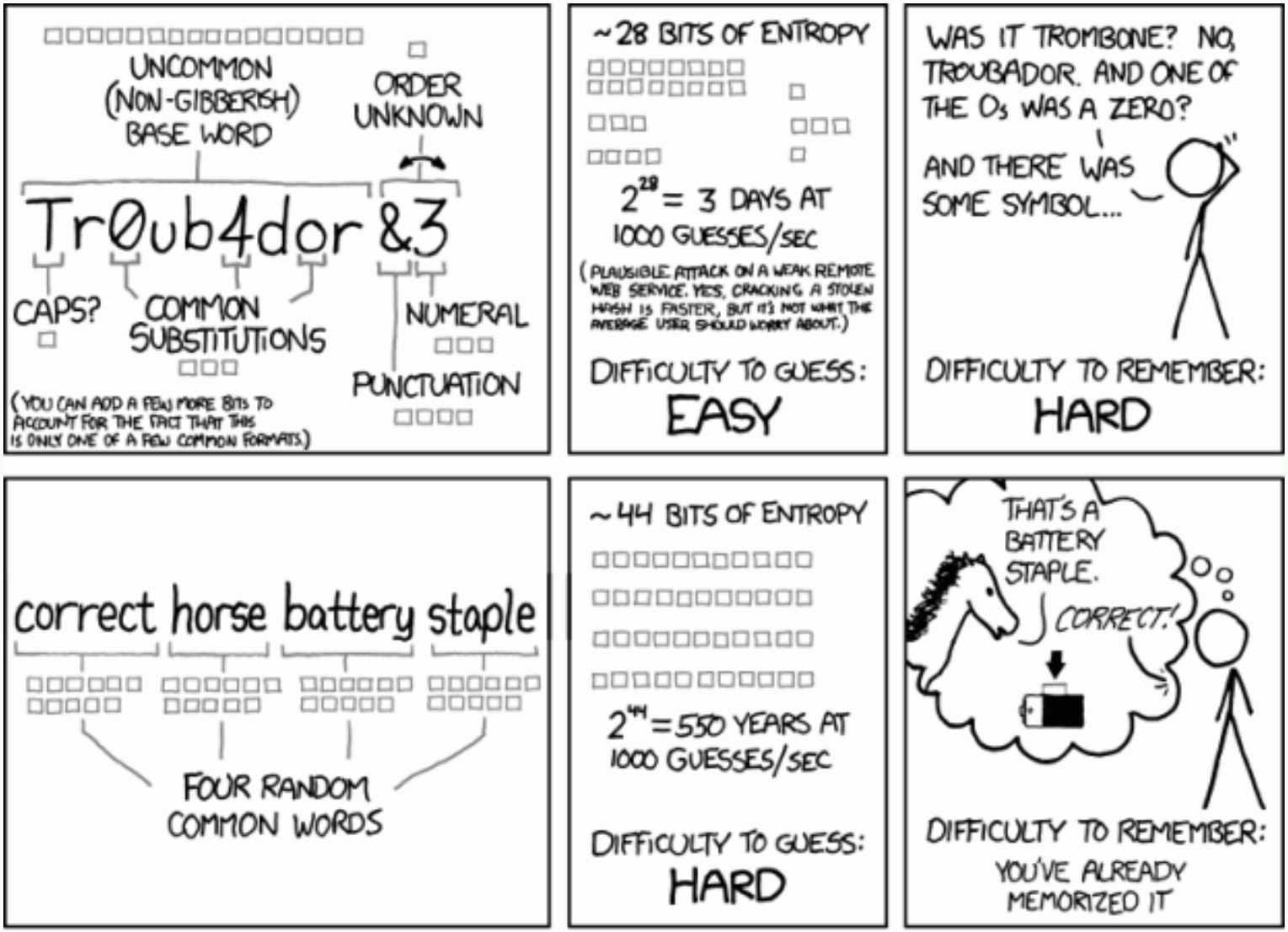
Κρυπτογραφία
ΠΜΣ Πληροφορική

Αν. Καθηγητής Κωνσταντίνος Πατσάκης

3 Νοεμβρίου 2021

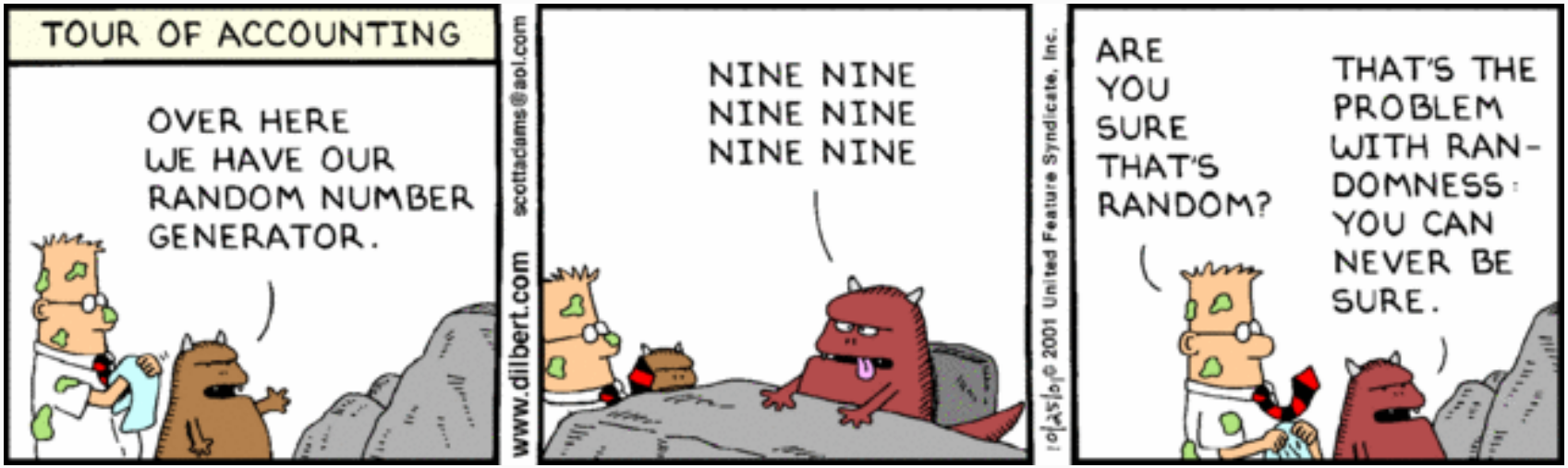
Τμήμα Πληροφορικής–Πανεπιστήμιο Πειραιώς

Κωδικοί

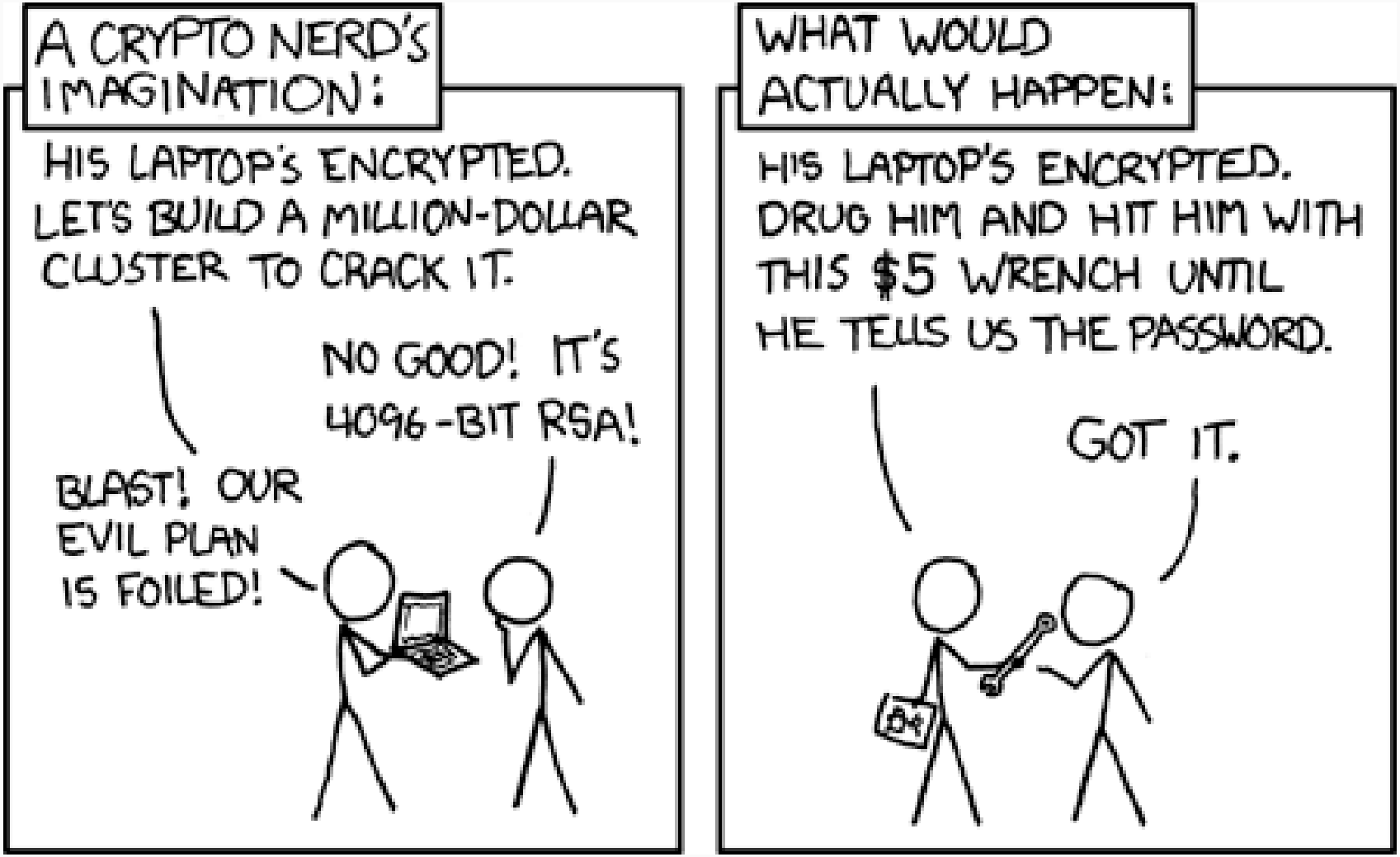

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
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.

Τυχαιότητα

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



Πραγματική ασφάλεια



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


HOW TO USE PGP TO VERIFY THAT AN EMAIL IS AUTHENTIC:
LOOK FOR THIS TEXT AT THE TOP:
REPLY
-----BEGIN PGP SIGNED MESSAGE-----
HASH: SHA256
HEY,
IF IT'S THERE, THE EMAIL IS PROBABLY FINE.


HEY, I JUST GOT HOME FROM THE PARTY
THE ONE WITH THE IRC FOLKS?
YEAH.
HOW WAS IT?
GOT TOO DRUNK. I SCREWED UP, BAD.
WHAT HAPPENED?
THERE WAS A GIRL. NO IDEA WHO SHE WAS. DON'T EVEN KNOW HER NAME. I WAS TOO DRUNK TO CARE.
AND WHAT, YOU SLEPT WITH HER?
NO.
I SIGNED HER PUBLIC KEY.
SHIT, MAN.

Διδασκαλία

5 Διαλέξεις

Τρόπος εξέτασης: Εργασίες

Επικοινωνία

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

Ερωτήσεις;