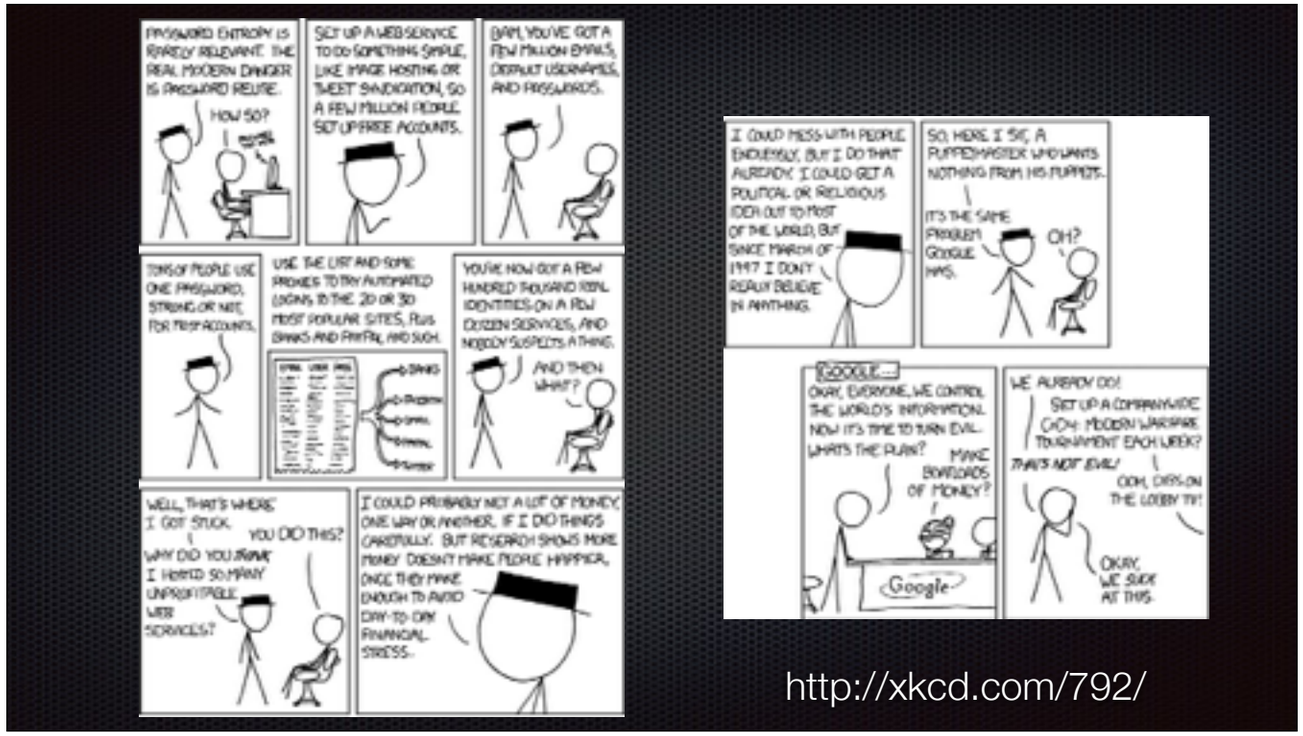


http://xkcd.com/792/

Cryptography & Privacy: Jcqtlqvo Bzcabewzbpg Agabmua

Bankim Tejani
IEEE-CEDA Austin
November 2014

@bankimtejani
tejani@alum.rpi.edu

Cryptography & Privacy: Building Trustworthy Systems

Bankim Tejani
IEEE-CS Austin
February 2014

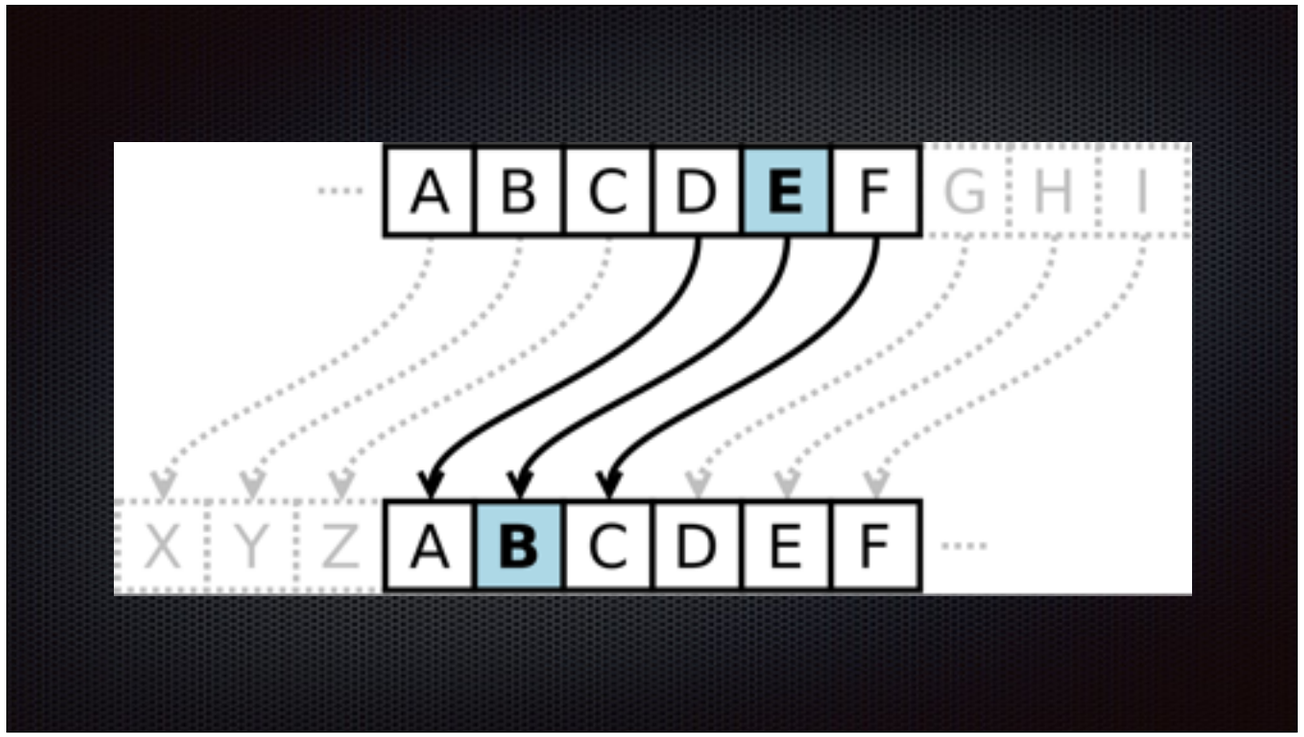
@bankimtejani
tejani@alum.rpi.edu

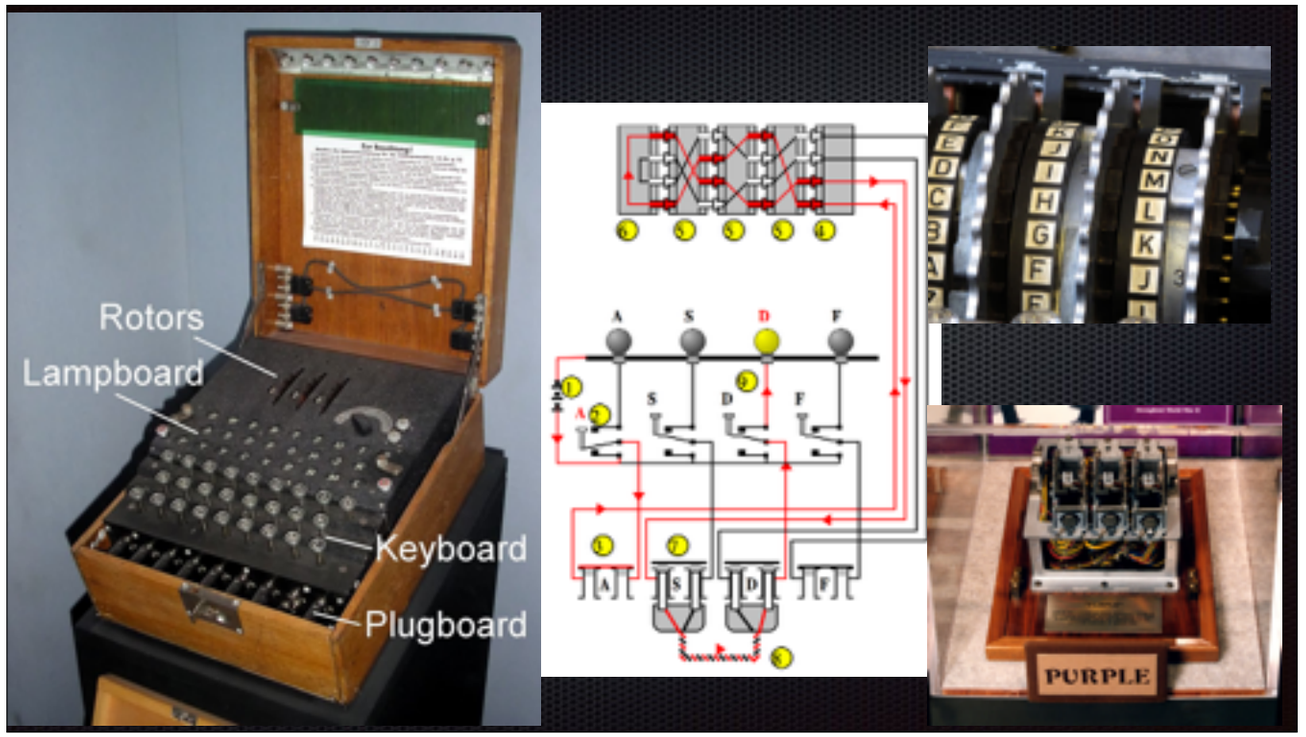
Goals & Objectives

- Cryptography fundamentals
- Privacy fundamentals
- Building systems with cryptography and privacy
- Preventing common mistakes
- Compliance and obligation

Em kiv xzwbmkb bpqa qvnwzuibqwv jmbbmz, bpca xzwbmkbqvo wczamtdma ia emtt. Bw lw aw, em ucab nqzab cvlmzabivl wcz wjtqoibqwva, zqasa, ivl zmycqzmumvba izwcvl libi xzwbmkbqwv. Em vmml i jmbbmz cvlmzabivlqvo wn kzgxbwozixpg, bpm mfxmkbml bmkpvwtwoqkit awtcbqwv. Em vmml bw cvlmzabivl bpm tmoit quxtqkibqwva wn pwtlqvo & uiqvbiqvqvo xzqdibm libi. Ivl em vmml bw kwvaqlmz wcz wjtqoibqwva izwcvl kcabwumz bzcab qv bpm iom wn vibqwvit qvbmttqomvkm, axgqvo, ivl bpm VAI.

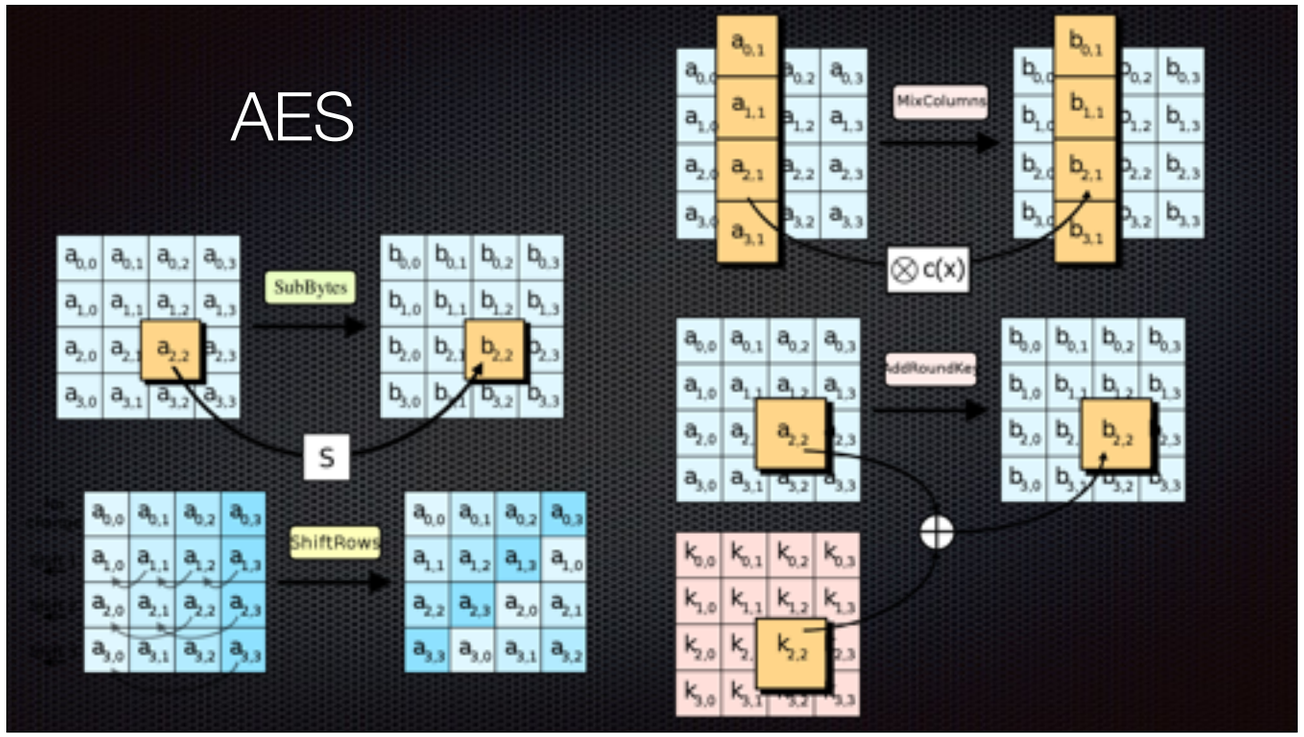
We can protect this information better, thus protecting ourselves as well. To do so, we must first understand our obligations, risks, and requirements around data protection. We need a better understanding of cryptography, the expected technological solution. We need to understand the legal implications of holding & maintaining private data. And we need to consider our obligations around customer trust in the age of national intelligence, spying, and the NSA.


A B C D E F G H I
X Y Z A B C D E F


Rotors
Lampboard
Keyboard
Plugboard
PURPLE

Cryptography Basics

- Cipher: a secret or disguised way of writing; a code
  - Ciphertext
- Secret key types
  - Symmetric
  - Asymmetric (public/ private)
- Key size
- Streaming
- Chaining
- Algorithmic quality / strength (trustworthiness??)
- Lifecycle?


AES
SubBytes
S
ShiftRows
MixColumns
⊗ c(x)

Password123$

- Caesarian-8: `Xiaaewzl123$`
- MD5: `5cbcf07e36fe37142b407ace0211cbf7`
- SHA1:
  `62d5a7eab7c13e99e355dd05b0377a6d01a8fa99`
- SHA512:
  `5a93a5e3ac9fb660046a11d20d6e90a9659f03f2`
  `9f9a29c056291aa7a1b039bccc71822e17619715`
  `b2209cb07cc8d807fb8f5c2ba9f56150cd43cf0e`
  `1b9719b5`

Password123$

- PGP (+Base64):

```
hQEMA/aXN+dLitihAQf/dk9KOM/
Us8Cs4UiJmcfgONL2CVO6Z6V1RDDOOW1akU5mHDfn8qovJpZJQd/
iVpS6DnOYq6rMjDqTnQAO4XeNZPD38ojdMIYIx39slxjVCtINgbWW5DvFx5j
+Oj/+lA9slLOA+1bw4zio8kQJhAuPZv74+3eVKuxOR3Wn/
MLYlApzfrFjJq28i8YrOI2dHpHOmbYepFwgDWGWQ6aleqvgfcv58evOBIjhOL
EiHYvpYS8KK11SicRiBnhAPV/8Ix
+6aupCVGF9O7GV2dBOWUFPiZulvvVRl68Hnxa6nTSJO2ryU7FYYNay2xgRTRA
frmgqkOtFuh9PwU67l6Ja86p/
GNLAigHd6o4fgs9UQwkwIhAiCLL2Ev2hQ43+hXFWpsAhO8pE
+dAsrSIBAyOEZ74tiz3Ny4BzkfOL8wTvbgDeZH7UljJ+rP/
imLY2QqIv8mUFOMtpvdBwhkZOvFgJQeI3PWnzjIrCZLzwkoxr7dW8GJpet4E7
wi9D/HBd7rRBt13fefn91ykHaeT4+eb3Gj8QeIC5I1LX8gYj8HlyJjOSqcLu
+PsE8NXnlHOHHc7uk9OnOgbQwebxlyQBbAtOBwPNhBOh9mhyBsOVP3rYIbSLR
Ct4wm9i3IqioIgMKIkoHRO4/hzJ6ZbEkUw6PP1ukMkipn
+w7ZNAzLCMNZUdEfwNOM6souQsdYw8HBqTNcgX4+6katGXlFkZ/
45h1KZrX7qchUNIUzws/D4jjLUnL2Dz4wCdSsVtywROX8Ys/
VxZDlFxCyGtvyQ29Y3bZWIdGg==
```

Cryptographic Attacks

- Brute force
- Frequency analysis
- Key recovery
- Cryptanalysis
- Collisions
- Rainbow tables
- Key management
- Software
- Experience

Privacy

What does it mean to you?

Privacy

1.

    1.1. the quality or state of being apart from company or observation : seclusion

    1.2. freedom from unauthorized intrusion <one's right to privacy>

2. archaic : a place of seclusion

3.

    3.1. secrecy

    3.2. a private matter : secret

Private Data Types

- Personally Identifiable Information (PII)
- PCI (Payment Card Industry) data
- Intellectual property
- Business data
- Financial data
- Identifiers - SSN,
- Passwords, tokens, keys
- Sessions
- Certificates

Privacy Requirements

- Protect from unauthorized users?
  - Who are they?
- Protect for how long?
- Privacy Act of 1974 (US)
- Foreign privacy laws
- Data-specific regulations

How do we build privacy in?

Relevant Systems

- Antennas and Propagation
- Circuits and Systems
- Computer
- Electron Devices
- Microwave Theory and Techniques
- Solid-State Circuits


Place
Speedpass
HERE
Speedpass


nest
COOLING
72
75
nest
2:17 PM
HOUSTON, TX
82°
IN 25 MIN
72
75
DOWNSTAIRS
UPSTAIRS


shutterstock
VISA

Password Storage & Protection

Password Storage & Protection

```
User record {
 userid
 pwhash
 attributes
}
```

Password Storage & Protection

```
User record {
 userid
 pwhash
 attributes
}
```

```
User record {
 userid
 pwhash
 salt
 attributes
}
```

Password Storage & Protection

```
User record {
 userid
 pwhash
 attributes
}
```

```
User record {
 userid
 pwhash
 salt
 attributes
}
```

```
User record {
 userid
 pwhash
 salt
 algorithm
 attributes
}
```

Password Storage & Protection

```
User record {
 userid
 user attributes
}
```

```
Passwords {
 userid
 pwhash
 salt
 algorithm
 status
  [active,expired]
 lastUsedTime
}
```

Password Storage & Protection

- Hashing
  - One-way
  - Salt
  - Slow
  - Keys & signing
- Attacks
  - Rainbow tables
  - Brute force
  - Password dumps

http://crackstation.net/hashing-security.htm

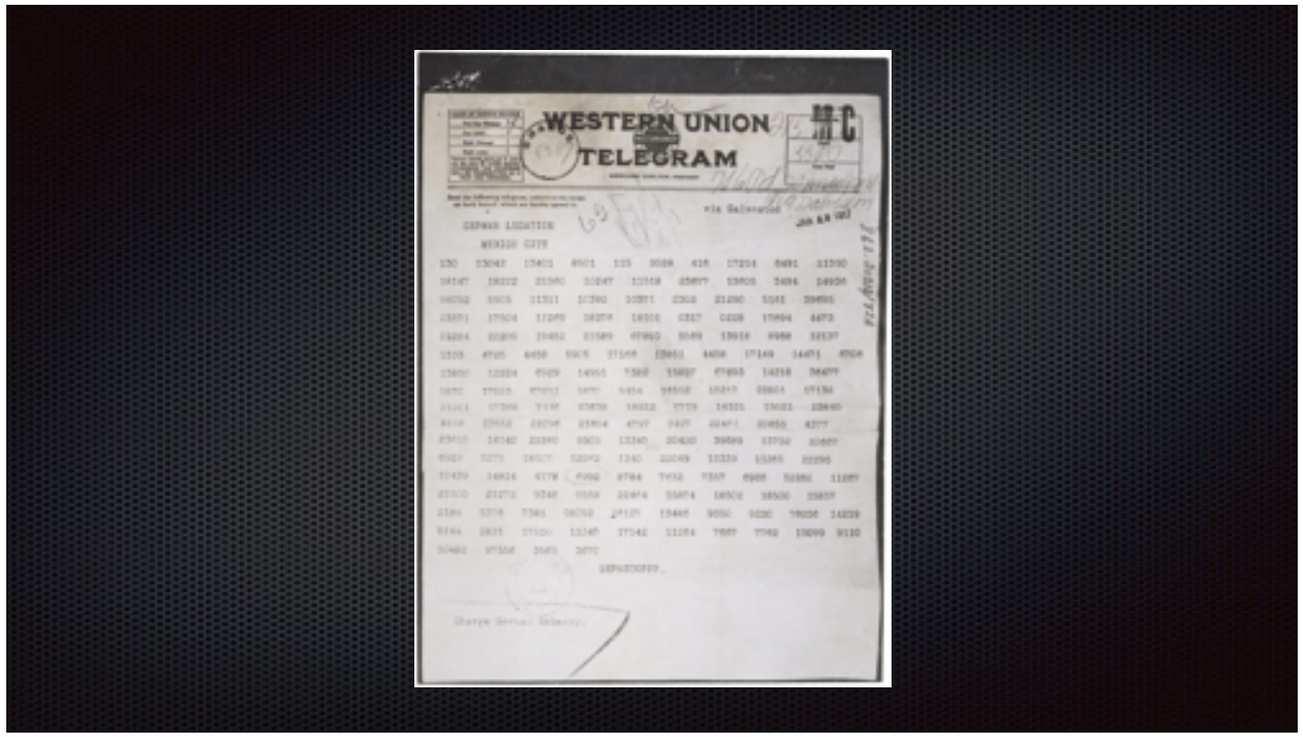
Password Storage & Protection

- Use:
  - SHA-256 or better
  - bcrypt
  - PBKDF2
  - SecureRandom, CSRNGs
- Don’t use:
  - MD5
  - SHA-1
  - Fixed salts
  - PRNGs

Core Principles

- Know your data
- Use vetted algorithms
- Plan for algorithmic changes
- Key management, rotation, expiration
- Data migration on key rotation
- Data deletion, expiration
- Authorized use
- Audit trails & compliance
- Supporting Infrastructure

Notable Failures



http://en.wikipedia.org/wiki/Zimmermann_Telegram


Place
Speedpass
HERE
Speedpass

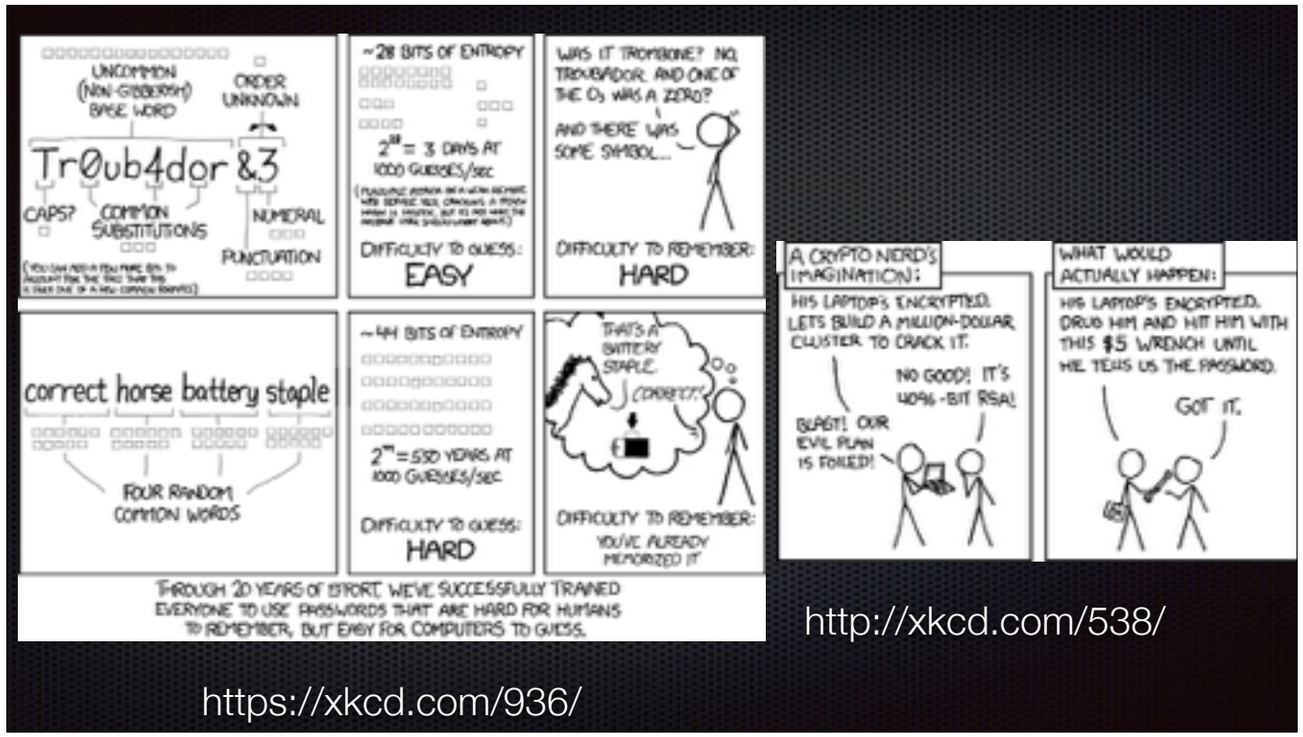
- Prof. Aviel D. Rubin, Adam Stubblefield, Matthew Green, Stephen Bono, and $3k
- Broke encryption on RFID chipset used by 2005 Ford Escape, Exxon SpeedPass, others
- http://www.nytimes.com/2005/01/29/national/29key.html

Sony - 2011

“an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email address, birthdate, PlayStation Network/ Qriocity password and login, and handle/PSN online ID. It is also possible that your profile data, including purchase history and billing address (city, state, zip), and your PlayStation Network/Qriocity password security answers may have been obtained... While there is no evidence at this time that credit card data was taken, we cannot rule out the possibility.”

Future Looking Trends

- What algorithms do we trust?
- Open selection
- Infinite compute & infinite storage
- Homomorphic data encryption



https://xkcd.com/936/

http://xkcd.com/538/

Thoughts?

http://en.wikipedia.org/wiki/Kryptos