

<http://xkcd.com/792/>

Cryptography & Privacy: Jcqtqvo Bzcabewzbpq 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

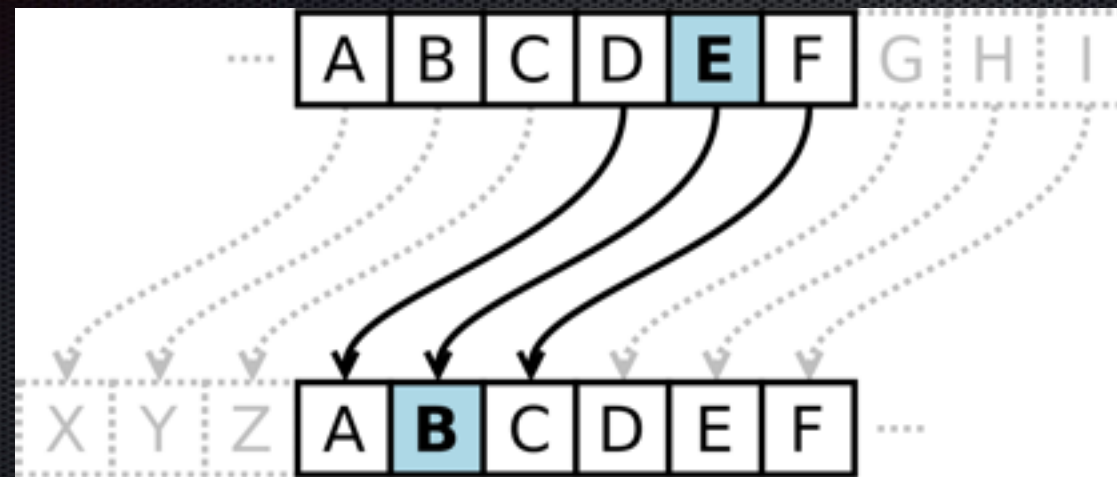
@bankimtejani
tejani@alum.rpi.edu

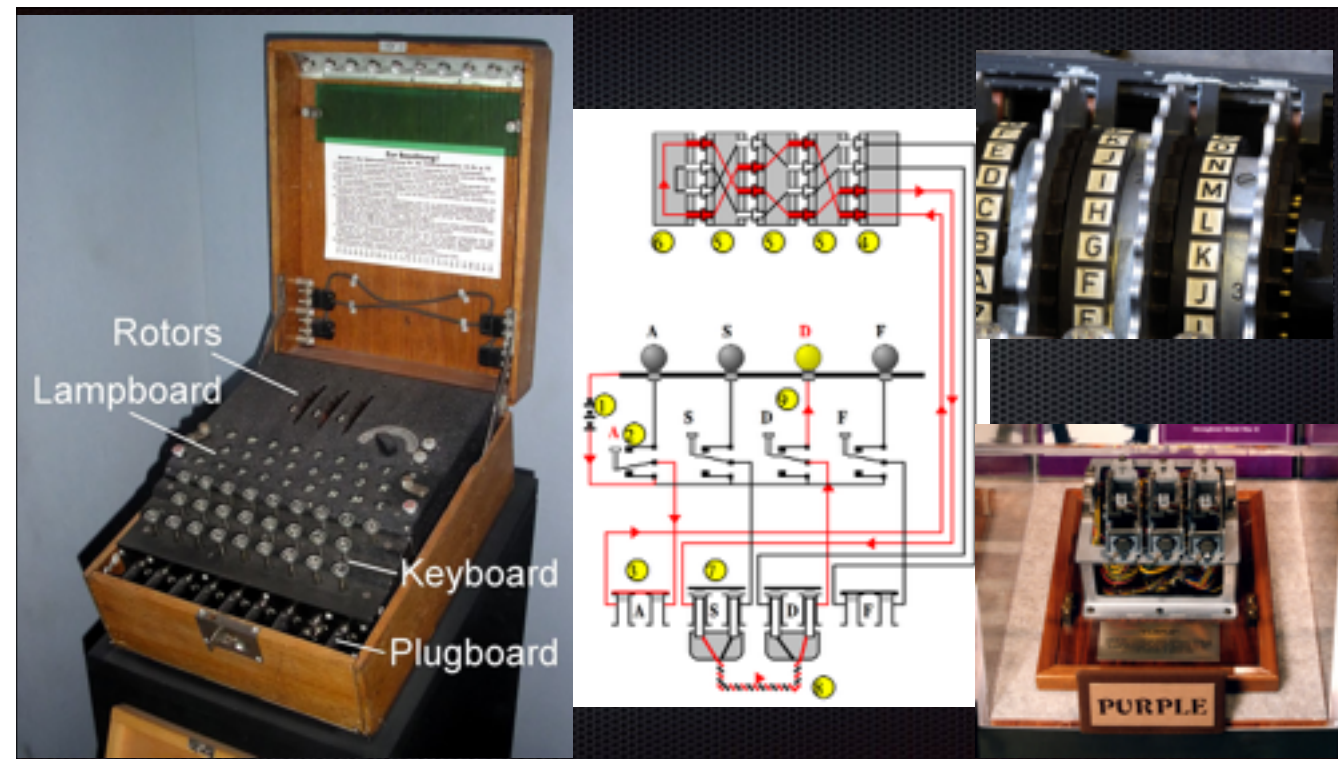
Goals & Objectives

- 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 bmkpwtwoqkit awtcbqwv. Em vmml bw
cvlmzabivl bpm tmoit quxtqkibqwva wn pwtlqvo &
uiqvbiqvqvo xzqdibm libi. Iv em vmml bw kwvaqlmz
wcz wjtqoibqwva izwcvl kcabwumz bzcab qv bpm iom
wn vibqwwit qvbmmtqomvkm, 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.

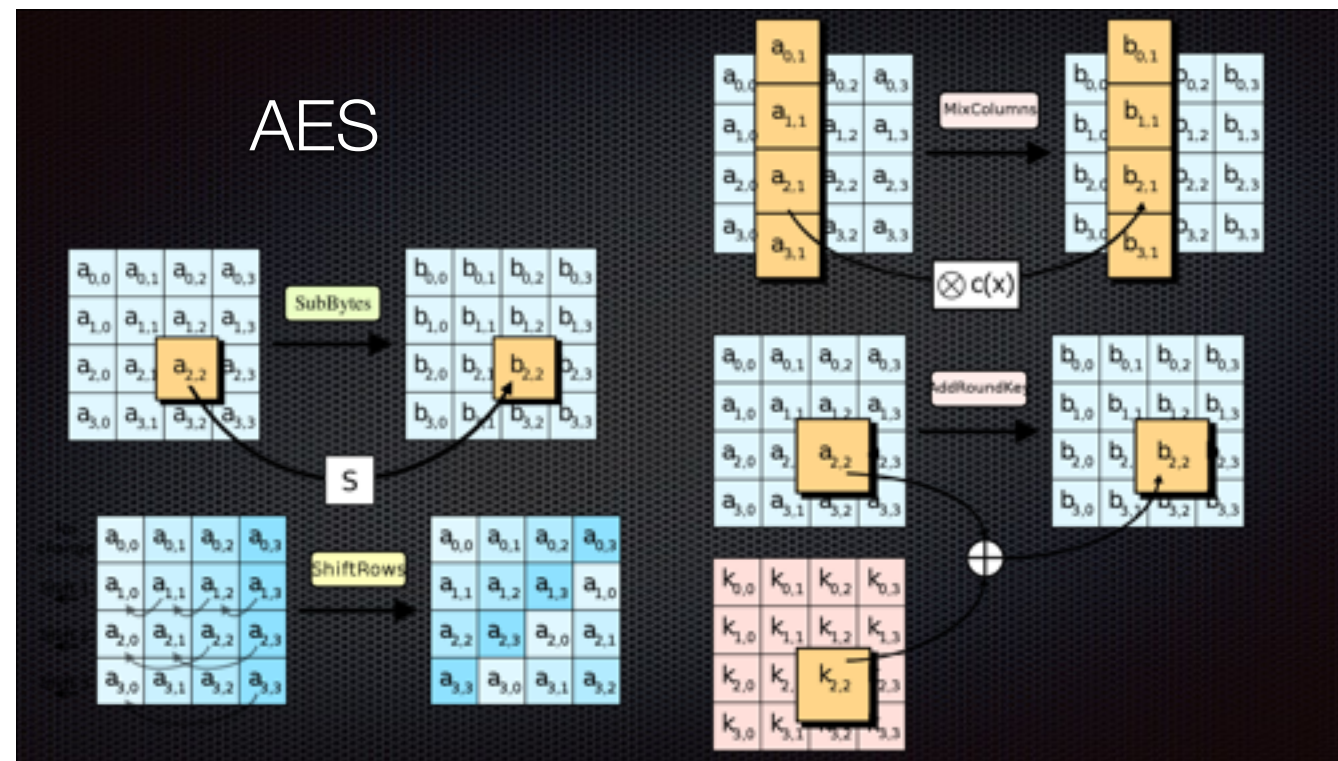




Cryptography Basics

- 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



Password123\$

- Caesarian-8: Xiaaewz1123\$
- MD5: 5cbcf07e36fe37142b407ace0211cbf7
- SHA1:
62d5a7eab7c13e99e355dd05b0377a6d01a8fa99
- SHA512:
5a93a5e3ac9fb660046a11d20d6e90a9659f03f2
9f9a29c056291aa7a1b039bccc71822e17619715
b2209cb07cc8d807fb8f5c2ba9f56150cd43cf0e
1b9719b5

Password123\$

▪ PGP (+Base64):
hQEMA/aXN+dLitihAQf/dk9KOM/
Us8Cs4UiJmcfg0NL2CV06Z6V1RDD00W1aku5mHDFn8govJpZJQd/
iVpS6Dn0Yq6rMjDqTnQA04XenZPD38ojdMIYIx39s1xjVctINGbWW5DvFx5j
+0j/+1A9s1LOA+1bw4zio8kQJhAuPZv74+3eVKux0R3Wn/
MLY1ApzfrFjJq28i8Yr0I2dHpH0mbYepFwgDWGwQ6a1eqvgfcv58ev0BIjh0L
EiHYvpYS8KK11SicRiBnhAPV/8Ix
+6aupCVGF907GV2dBOWUFPiZu1vvVR168Hnxa6nTSJ02ryU7FYYNay2xgRTRA
frmgqkotFuh9PwU6716Ja86p/
GNLAighd6o4fgs9UQkwIhAiCLL2Ev2hQ43+hxFWpsAh08pE
+dAsrSIBay0EZ74tiz3Ny4BzkfOL8wTvbGDeZH7U1jJ+rP/
imLY2QqIv8mUFOMtpvdBwhkZ0vFgJQeI3PwnzjIrCZLzwkoxr7dw8GJpet4E7
wi9D/HBd7rRBt13fefn91ykHaet4+eb3Gj8QeIC5I1LX8gYj8HlyJjOSqCLu
+PSE8NXn1H0HHc7uk9on0gbQwebxlyQBbAtOBwPNhB0h9mhyBSOVP3rYIbSLR
Ct4wm9i3IqioIgMKIkoHR04/hzJ6ZbEkUw6PP1ukMkipn
+w7ZNAZLCMNZUdEfwN0M6souQsdYw8HBqTncgX4+6katGX1Fkz/
45h1KZrx7qchUNIuzws/D4jjLUnL2Dz4wCdSsvtywROX8Ys/
VxZD1FxCyGtvvyQ29Y3bZWIdGg==

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











Password Storage & Protection

Password Storage & Protection

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

Password Storage & Protection

User record {	User record {
userid	userid
pwhash	pwhash
attributes	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

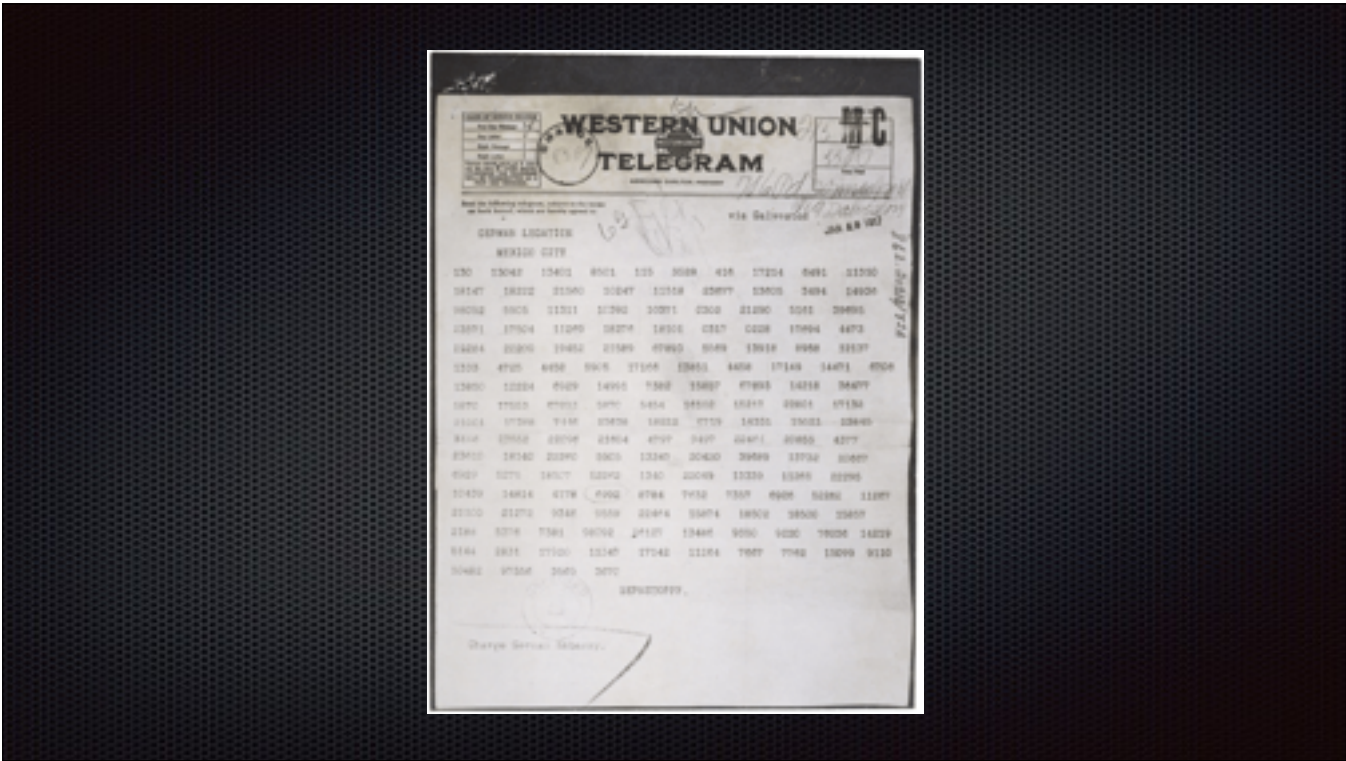
▪ Don't use:

- 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



- 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

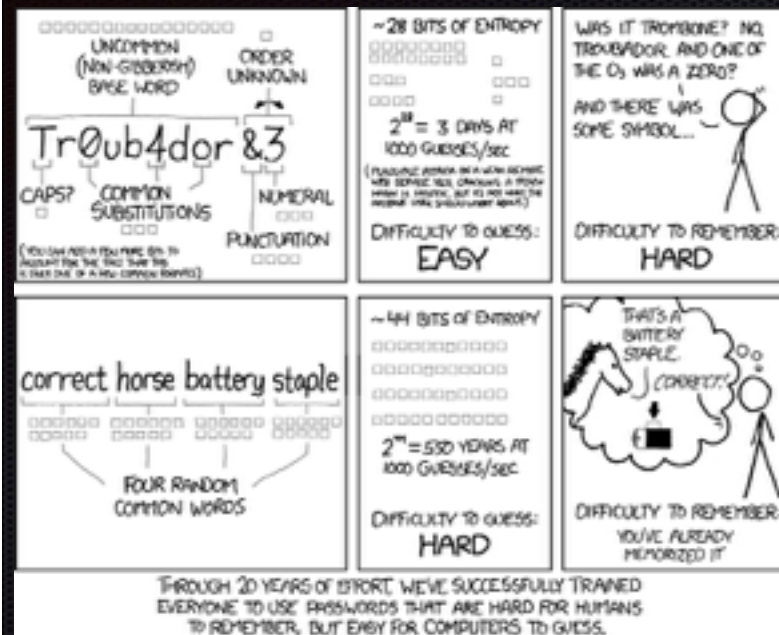
“an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email address, birthdate, PlayStation Network/Qriocity password and login, and handle/PSN online ID. It is also possible that your profile data, including purchase history and 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



<http://xkcd.com/538/>

<https://xkcd.com/936/>

Thoughts?



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