Admin:

Psst #1 due Monday

Today:

- Encryption
- One-time Pad
- Hash Functions (if time...)
  - definitions
  - Random Oracle Model

Readings:

(highly recommended)

Katz/Lindell Chaps 1, 2, 3, 5

News:

- Anthem data breach (80M customers; $100M; govt employees)
- 100 banks/30 countries/$100M or $1B? ATM’s, etc. Carbanak ring
- PC spyware—rewrites disk firmware. “Equation Group”
- Netgear wireless routers reveal admin password
Encryption

Goal: confidentiality of transmitted (or stored) message

Parties: Alice, Bob "good guys"
Eve "eavesdropper, adversary"

Alice  \[ M \]  \[\rightarrow\] Bob
\[\text{Eve}\]

\[ M = \text{transmitted message}\]

In basic picture above, there is nothing to distinguish Bob from Eve; they both receive message.

Could have dedicated circuits (e.g., helium-filled pipes containing fiber optic cable,...?) or steganography.

Crypto approach: • Bob knows a key \( K \) that Eve doesn't (Eve knows system)
  • Alice can encrypt message so that knowledge of \( K \) allows decryption.
  • Eve hears ciphertext, but learns "nothing" about \( M \).
With classical (non public key) crypto, Alice & Bob both know key $K$. Shared symmetric key.

**Algorithms:**

- $K \leftarrow \text{Gen}(1^\lambda)$  
  \(\lambda\) given in unary

- $C \leftarrow \text{Enc}(K, M)$  
  encrypt message $M$ with key $K$, result is ciphertext $C$

- $M = \text{Dec}(K, C)$  
  decrypt $C$ using $K$ to obtain $M$

(Note Katz/Lindell convention: “$\leftarrow$” for randomized operations, “$=$” for deterministic ones. Often $\leftarrow_R$ or $\leftarrow_S$ is used for randomized operation.)

**Setup:**

Someone computes $K \leftarrow \text{Gen}(1^\lambda)$

(Someone may be Alice or Bob)

Ensures that Alice & Bob both have $K$ (and Eve doesn’t)  \(\text{how! ?}\)

**Communication:**

\[
K \quad \text{Alice} \quad C \leftarrow \text{Enc}(K, M) \quad \text{Bob} \quad K \\
C \leftarrow \text{Enc}(K, M) \quad \text{Eve} \quad M = \text{Dec}(K, C) \quad ???
\]
Security objective:

Eve can't distinguish \( \text{Enc}(K, M_1) \) from \( \text{Enc}(K, M_2) \), even if she knows (or chooses) \( M_1 \) and \( M_2 \) (\( M_1 \neq M_2 \)) (of the same length).

(Encryption typically does not hide message length.)

Attacks:
- Known ciphertext
- Known CT/PT pairs
- Chosen PT
- Chosen CT

\[ \{ \text{Ciphertext indistinguishability} \}
\{ \text{Semantic security} \]
One-Time Pad (OTP)

- Vernam 1917 paper-tape based, Patent.
- Message, key, and ciphertext have same length (\( \lambda \) bits)
- Key \( K \) also called pad; it is random & known only to Alice & Bob.
  (Note: used by spies, key written on small pad...)
- **Enc**: \( M = 101100... \) (binary string)
  \[ \oplus K = 011010... \] (mod-2 each column)
  \[ C = 110110... \]

- **Dec**: Just add \( K \) again:
  \[ (m_i \oplus k_i) \oplus k_i = m_i \oplus (k_i \oplus k_i) \]
  \[ = m_i \oplus 0 = m_i \]

**Joke**: (Desmedt Crypto rump session)
OTP is weak, it only encrypts \( \frac{1}{2} \) the bits! Leakage!
Better to change them all!

**Theorem**: OTP is unconditionally secure.
(Secure against Eve with unlimited computing power.)
\( \text{a.k.a. information-theoretically secure.} \)
One-Time Pad (Security proof)

\[ M = 101100 \ldots \quad (\lambda\text{-bit string}) \]
\[ K = 011010 \ldots \quad (\text{xor } \lambda\text{-bit "pad" (key)}) \]
\[ C = 110110 \ldots \quad (\lambda\text{-bit ciphertext}) \]
\[ M = 101100 \ldots \]

\[ (M \oplus K) \oplus K = M \oplus (k \oplus k) = M \oplus 0^n = M \]

OTP is information-theoretically secure = Eve

can not break scheme, even with unlimited computing power

(Compare to computationally secure: requires assumption that Eve has limited computing power (e.g., can't factor large numbers).)

Model Eve's uncertainty via probabilities

\[ P(M) = \text{Eve's prior probability that message is } M \]
\[ P(M|C) = \text{Eve's posterior probability that message is } M, \text{ after having seen ciphertext } C. \]

Theorem: For OTP, \[ P(M) = P(M|C) \]

\[ \Rightarrow \text{"Eve learns nothing by seeing } C." \]
Proof:

Assume $|M| = |K| = |C| = \lambda$.

$$P(k) = 2^{-\lambda} \quad \text{(all } \lambda\text{-bit keys equally likely)}$$

Lemma: $P(c \mid M) = 2^{-\lambda}$

$$P(c \mid M) = \text{Prob of C, given M}$$
$$= \text{Prob that } K = C \oplus M$$
$$= 2^{-\lambda}.$$ 

$$P(C) = \text{Probability of seeing ciphertext C}$$
$$= \sum_{M} P(c \mid M) \cdot P(M)$$
$$= \sum_{M} 2^{-\lambda} \cdot P(M)$$
$$= 2^{-\lambda} \sum_{M} P(M)$$
$$= 2^{-\lambda} \cdot 1 = 2^{-\lambda} \quad \text{(uniform)}$$

$$P(M \mid C) = \text{Prob of M, after seeing C (posterior)}$$
$$= \frac{P(c \mid M) \cdot P(M)}{P(c)} \quad \text{(Bayes' Rule)}$$
$$= \frac{2^{-\lambda} \cdot P(M)}{2^{-\lambda}}$$
$$= P(M) \quad \text{QED}$$

This is perfect secrecy (except for length $\lambda$ of $M$).
Notes:

Users need to:
- generate large secrets
- share them securely \{usability??\}
- keep them secret
- avoid re-using them (google "Venona")

\[ C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K) \]
\[ = M_1 \oplus M_2 \]
from which you can derive
\[ M_1, M_2 \] often.

Theorem: OTP is malleable.

(That is, changing ciphertext bits causes corresponding bits of decrypted message to change.)

OTP does not provide any authentication of message contents or protection against modification ("mauling").
How to generate a random pad?

- Coins, Cards
- Dice
- Radioactive sources (old memory chips were susceptible to alpha particles)
- Microphone, Camera
- Hard disk speed variations
- Intel 82802 chip set
- User typing or mouse movements
- Lava lamp (lava lamp → camera)
- Alpern & Schneider:

  \[ A \rightarrow B \]

  Eve can't tell who transmits.
  A & B randomly transmit beeps.
  They can derive shared secret.

- Quantum Key Distribution

  Polarized light: \( \uparrow \leftrightarrow \downarrow \leftrightarrow \leftarrow \rightarrow \)

  Filters (A): \( \circ \circ \circ \circ \circ \circ \)

  (example filter)

  result: \( \uparrow \leftrightarrow \uparrow \leftrightarrow \downarrow \leftrightarrow \uparrow \leftrightarrow \downarrow \)

  or \( \uparrow \leftrightarrow \downarrow \leftrightarrow \uparrow \leftrightarrow \downarrow \leftrightarrow \uparrow \)

  A sends single photons, polarized randomly.
  B publicly announces filter choices.
  Then they know which bit they should have in common.

ref today's lecture on "Continuous Quantum Dice"

"Noise diodes"

\[ 5V \rightarrow A/D \rightarrow \text{bits} \]
Final project idea

smart phone app:

* generate pads using camera
* share pads when meet (a la “bump”)
* send confidential messages