6.857 - Network & Computer Security  

Reminder: Mon = 66-110 Wed = 56-114
http://courses.csail.mit.edu/6.857

Administrivia: Sign up online if you haven't yet.
Pset #1 now posted.
No recitation this week.

Today:  
☐ Finish material from lecture 1 (notes L1.5 - L1.8)
☐ Encryption
☐ Perfect secrecy
☐ One-time pad (OTP)

News:
{ "Traveling Light in a Time of Digital Thrift" NYT 2/11/12
"Ron was wrong, Whit is right" (Lenstra et al.) IACR eprint 2012/064, 2/14/12
"Freedom to Tinker: There's no need to panic over flawed keys" 2/15/12 by N. Heninger

Reading: (highly recommended)
Katz/Lindell chapters 1, 2, 3
Encryption

**Goal:** confidentiality of transmitted (or stored) message

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

![Diagram](image)

M = 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
- 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 $K$.

Algorithms:

$K \leftarrow \text{Gen}(1^\lambda)$  
*generate key of length $\lambda$  
($\lambda$ 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,  
\(\Rightarrow\) = for deterministic ones  
Often \(\leftarrow^R\) or \(\leftarrow^\ast\) 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)  
(how!?)

Communication:

$K \xrightarrow{} \text{Alice}$  

$C \xrightarrow{} \text{Enc}(K, M)$  

$\text{Bob} \xrightarrow{} K$  

$C \xrightarrow{} \text{Enc}(K, M)$  

???

Eve  

$M = \text{Dec}(K, C')$
Security objective:

Eve can't distinguish Enc$(K, M_1)$ from 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 \(\{\text{assumes } K \text{ is re-used} \}

chosen PT

chosen CT

...
One-Time Pad (OTP)

- Message, key, and ciphertext have same length (λ bits)
- Key K also called pad; it is random & known only to Alice & Bob.
  (Note: used by spies, key written on small pad...)
- **Enc:** \( M = 10\ 11\ 00 \ldots \) (binary string)
  \[ \oplus K = 01\ 10\ 10 \ldots \] (mod-2 each column)
  \[ C' = 11\ 01\ 10 \ldots \]
- **Dec:** Just add K again: \((m_i \oplus k_i) \oplus k_i = m_i\)

**Joke:** (Desmedt Crypt rump session)
OTP is weak, it only encrypts ½ the bits! leakage!
Better to change them all!

**Theorem:** OTP is unconditionally secure.
(Secure against Eve with unlimited computing power.)
aka, information-theoretically secure.
One-Time Pad (Security proof)

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

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

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

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

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

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

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

$P(k) = 2^{-\lambda}$  \hspace{1cm} (all $\lambda$-bit keys equally likely)

**Lemma:** $P(C|M) = 2^{-\lambda}$

$P(C|M) = \text{Prob of } C, \text{ given } M$

$= \text{Prob that } K = C \oplus M$

$= 2^{-\lambda}$.

$P(C) = \text{Probability of seeing ciphertext } C$

$= \sum_{M} P(C|M) \cdot P(M)$

$= \sum_{M} 2^{-\lambda} \cdot P(M)$

$= 2^{-\lambda} \sum_{M} P(M)$

$= 2^{-\lambda} \cdot 1 = 2^{-\lambda}$,  \hspace{1cm} (uniform)

$P(M|C) = \text{Prob of } M, \text{ after seeing } C \text{ (posterior)}$

$= \frac{P(C|M) \cdot P(M)}{P(C)} \hspace{1cm} \text{(Bayes' Rule)}$

$= \frac{2^{-\lambda} \cdot P(M)}{2^{-\lambda}}$

$= P(M)$  \hspace{1cm} QED$

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