Admin:
Pset #1 posted; see TAs if necessary re groups
due 2/12

Hudson talk today at 4 pm in 32-6882 re macbook bootkits

Today:

- Finish Killian talk
- Encryption
- One-time pad (OTP)
- Hash fun (start: if time...)

Reading:

Katz & Lindell Chaps. 1, 2, 3, 5 (recommended)
Encryption

Goal: confidentiality of transmitted (or stored) message

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

\[ \text{Alice} \rightarrow M \rightarrow \text{Bob} \]
\[ \text{Eve} \] \hspace{1cm} \text{communication channel} \]

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

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 optics, ...) 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:**

$K \leftarrow \text{Gen}(1^\lambda)$  \hspace{1cm} \text{generate key of length } \lambda \hspace{1cm} (\lambda \text{ given in unary})

$C \leftarrow \text{Enc}(K, M)$  \hspace{1cm} \text{encrypt message } M \text{ with key } K \hspace{1cm} \text{result is ciphertext } C$

$M = \text{Dec}(K, C)$  \hspace{1cm} \text{decrypt } C \text{ using } K \text{ to obtain } M$

(Note Katz/Lindell conventions: $\leftarrow$ for randomized operations, $\leftarrow^R$ or $\leftarrow^{\#}$ 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)  \hspace{1cm} \text{(how?)}

**Communication:**

- $K$ Alice $C \overset{\text{Enc}(K, M)}{\rightarrow}$ Bob $K$
- $C \overset{\text{Enc}(K, M)}{\rightarrow}$ 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

\{Ciphertext indistinguishability\}
\{Semantic security\}

Similar "game" def:

- Alice picks key \(K\)
- Alice tells Eve message length \(\lambda\)
- Eve makes up two messages \(M_1, M_2\) of length \(\lambda\)
- Alice flips a bit \(b\) \((b = 1 \text{ or } b = 2)\)
- Alice gives Enc(\(K,b, M_b\)) to Eve
- Eve produces guess \(\hat{b}\) for \(b\).
  Eve wins if \(\hat{b} = b\).

Eve's advantage is \(\text{Prob}(\hat{b} = b) - \frac{1}{2}\).

Advantage should go to zero as \(|K|\) increases.
E.g., "negligible" means goes to zero faster
than \(1/\text{poly}(n)\) where \(n\) = security parameter.
One-Time Pad (OTP)


- 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 nonsense) OTP is weak, it only encrypts 1/2 the bits! leakage! Better to change them all!

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

\[ M = 101100\ldots \quad (\text{\(\lambda\)-bit string}) \]
\[ K = 011010\ldots \quad (\text{xor \(\lambda\)-bit 'pad' (key)}) \]
\[ C = 110110\ldots \quad (\text{\(\lambda\)-bit ciphertext}) \]
\[ M = 101100\ldots \]
\[ (M \oplus K) \oplus K = M \oplus (K \oplus K) = M \oplus 0 = M \]

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, \( P(M) = P(M|C) \)

\( \equiv \) "Eve learns nothing by seeing \( C \)"
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)

$P(M|C) = \text{Prob of } M, \text{ after seeing } C$ (posterior)
$= \frac{P(C|M) \cdot P(M)}{P(C)}$ \hspace{1cm} (Bayes' Rule)
$= \frac{2^{-\lambda} \cdot P(M)}{2^{-\lambda}}$
$= P(M)$ \hspace{1cm} QED

This is perfect secrecy (except for length $\lambda$ of $M$).
Users need to
- generate large secrets
- share them securely
- 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").

**Note:** OTP analyzed in terms of bits (digital abstraction)

In reality, Eve hears waveforms, and 0 or 1 might look different than 1 or 0