6.857 - Network & Computer Security

2/15/12
L3.1

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

Administrivia: Sign up on line 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)

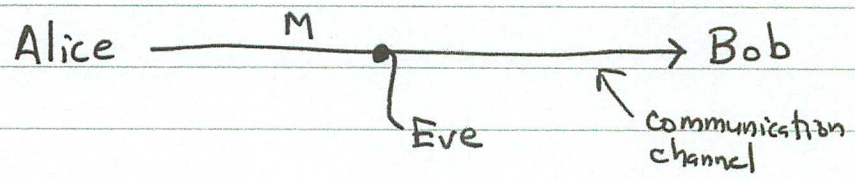
News:
- "Traveling Light in a Time of Digital Thievery" NYT 2/11/12
- "Ron was wrong, Whit is right" (Lenstra et al.) IACR eprint 2012/064, 2/14/12
- "Freedom to Tinker: There's no need to panic over factorable keys" 2/15/12 by N. Heninger

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"



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:

$K \leftarrow Gen(1^\lambda)$ — generate key of length λ (λ given in unary)

$C \leftarrow Enc(K, M)$ — encrypt message M with key K, result is ciphertext C

$M = Dec(K, C)$ — decrypt C using K to obtain M

(Note Katz/Lindell convention: "$\leftarrow$" for randomized operations, "$=$" for deterministic ones

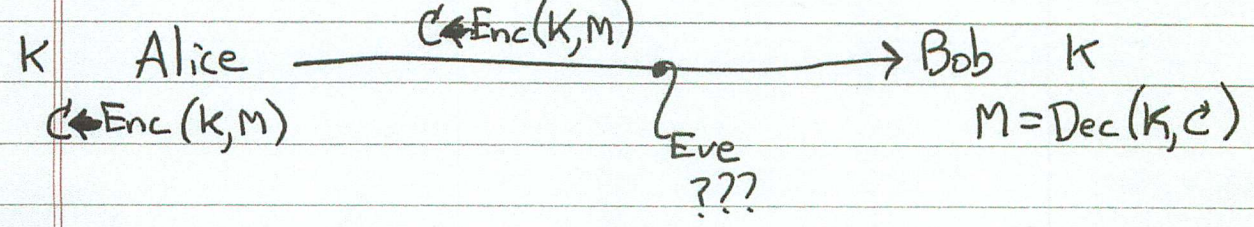
Often $\xleftarrow{R}$ or $\xleftarrow{\$}$ is used for randomized operation.)

Setup: Someone computes $K \leftarrow Gen(1^\lambda)$

(Someone may be Alice, or Bob)

Ensures that Alice & Bob both have K (and Eve doesn't) (how!?)

Communication:



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
- chosen PT
- chosen CT
- ...

} assumes K is re-used

One-Time Pad (OTP)

- Vernam 1917 paper-tape based. Patent.

- 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: $M = 101100\ldots$ (binary string)
  $\oplus\ K = 011010\ldots$ (mod-2 each column)
  $C = 110110\ldots$

- Dec: Just add K again: $(m_i \oplus k_i) \oplus k_i = m_i$

Joke: (Desmedt Crypto rump session)
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.)
a.k.a. information-theoretically secure.

One-Time Pad (Security proof)

Enc ⇓
$M = 1011000\cdots$ (λ-bit string)
$\oplus\ K = 0110100\cdots$ (xor λ-bit "pad" (key))
$C = 1101100\cdots$ (λ-bit ciphertext)

Dec ⇓
$\oplus\ K = 0110100\cdots$
$M = 1011000\cdots$

$$(M \oplus K) \oplus K = M \oplus (K \oplus K) = M \oplus 0^{\lambda} = M$$

OTP is <u>information-theoretically secure</u> = Eve can not break scheme, even with unlimited computing power

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

Model Eve's uncertainty via probabilities

$P(M)$ = Eve's prior probability that message is M

$P(M|C)$ = Eve's posterior probability that message is M, after having seen ciphertext C.

<u>Theorem:</u> For OTP, $P(M) = P(M|C)$

$\equiv$ "Eve learns <u>nothing</u> by seeing C"

Proof:

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

$P(K) = 2^{-\lambda}$ (all λ-bit keys equally likely)

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

$P(c|M)$ = Prob of C, given M

= Prob that $K = C \oplus M$

$= 2^{-\lambda}$.

$P(C)$ = Probability of seeing ciphertext C

$$= \sum_M P(C|M) \cdot P(M)$$

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

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

$= 2^{-\lambda} \cdot 1 = 2^{-\lambda}$. (uniform)

$P(M|C)$ = Prob of M, after seeing C (posterior)

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

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

$= P(M)$ QED

This is <u>perfect secrecy</u> (except for length λ of M).