TOPIC: 6.857

DATE: 2/10/16

FILE UNDER:

Admin:

Pset #1 posted; see TAs if necessary re groups
due 2/22

Hudson talk today at 4pm in 32-G882 re macbook bootkits

Today:

- Finish Killian talk
- Encryption
- One-time pad (OTP)
- Hash fns (start; if time...)

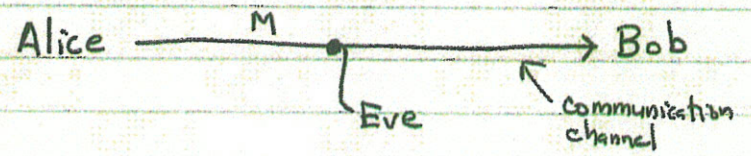
Reading:

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

Encryption

Goal: confidentiality of transmitted (or stored) message

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



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

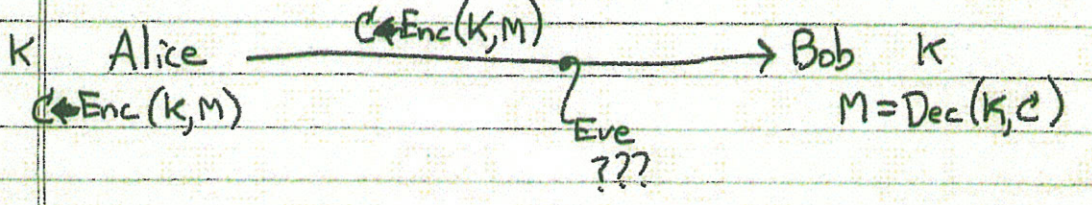
$C \leftarrow Enc(K, M)$ encrypt message M with key K, result is ciphertext C

$M = Dec(K, C)$ 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

{ ciphertext indistinguishability
{ semantic security

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

Eve's advantage is $Prob(\hat{b} = b) - 1/2$

Advantage should go to zero as $|K|$ increases.
e.g. "negligible" means goes to zero faster than $1/poly(n)$ where n = security parameter.

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: $(m_i \oplus k_i) \oplus k_i = m_i \oplus (k_i \oplus k_i)$
  $= m_i \oplus 0 = m_i$

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 ↓
$M = 1\,0\,1\,1\,0\,0\,\cdots$ (λ-bit string)
$\oplus\ K = 0\,1\,1\,0\,1\,0\,\cdots$ (xor λ-bit "pad" (key))
$C = 1\,1\,0\,1\,1\,0\,\cdots$ (λ-bit ciphertext)

Dec ↓
$\oplus\ K = 0\,1\,1\,0\,1\,0\,\cdots$
$M = 1\,0\,1\,1\,0\,0\,\cdots$

$(M \oplus K) \oplus K = M \oplus (K \oplus K) = M \oplus \vec{0} = M$

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)

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

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

$= P(M)$ QED

This is perfect secrecy (except for length λ of M).

Notes:

Users need to
- generate large secrets
- share them securely
- keep them secret

} usability??

- 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.

Project 1 Venona

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+1 might look different than 1+0