TOPIC: 6.857 - Computer & Network Security

DATE: 2/12/14

FILE UNDER:

PAGE: L3.1

Admin:

Pset #1 posted: see TA if you don't have assigned group.

Recitation starts this week (Fri, 4-270, 11am)

Project idea:

"audio & security" possibilities

1. cryptanalysis by sound: http://www.cs.tau.ac.il/~tromer/acoustic
2. cross-platform malware communicates with sound slashdot 10/31/13
3. company illiri (see slashdot 7/23/13)

Today:

- Encryption
- Perfect Secrecy
- One-Time Pad (OTP)

Readings:

(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

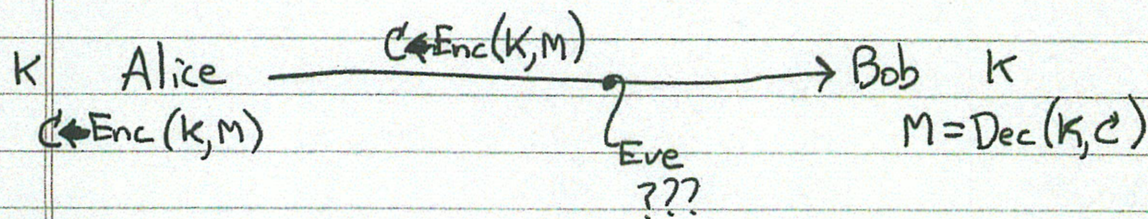
$M = Dec(K, C)$ — decrypt C using K to obtain M

(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

$$\left.\begin{array}{l}\text{known CT/PT pairs}\\ \text{chosen PT}\\ \text{chosen CT}\end{array}\right\}\text{ assumes } K \text{ is re-used}$$

...

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:
$$\begin{array}{rl} M = & 101100\cdots \\ \oplus\ K = & 011010\cdots \\ \hline C = & 110110\cdots \end{array}$$
(binary string)
(mod-2 each column)

- 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.

TOPIC:

DATE:

FILE UNDER:

One-Time Pad (Security proof)

$$
\begin{array}{lll}
 & M = 1\,0\,1\,1\,0\,0 \cdots & (\lambda\text{-bit string}) \\
\text{Enc} \downarrow\; \oplus & K = 0\,1\,1\,0\,1\,0 \cdots & (\text{xor } \lambda\text{-bit "pad" (key)}) \\
\hline
 & C = 1\,1\,0\,1\,1\,0 \cdots & (\lambda\text{-bit ciphertext}) \\
\text{Dec} \downarrow\; \oplus & K = 0\,1\,1\,0\,1\,0 \cdots & \\
\hline
 & M = 1\,0\,1\,1\,0\,0 \cdots &
\end{array}
$$

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

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

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

TOPIC:

DATE:

FILE UNDER:

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).

TOPIC: DATE:

FILE UNDER: PAGE L4.4

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.

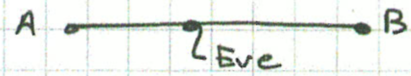
Theorem: OTP is malleable.

(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").

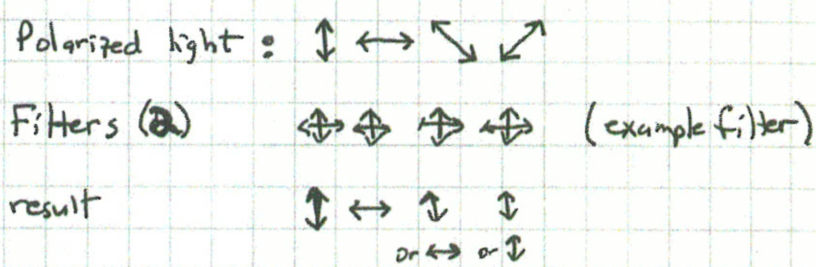
How to generate a random pad?

- Coins
- 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
- Lavarand (lava lamp ⇒ camera)
- Alpern & Schneider:



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

- Quantum Key Distribution



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

~~a ref today's lecture on Certifiable Quantum Dice~~

- "Noise diodes"