TOPIC: 6.857

DATE: 2/17/15

FILE UNDER:

PAGE: L04.1

Admin: Pset #1 due Monday

Today:

- Encryption
- One-time Pad
- Hash Functions (start if time...)
  - definitions
  - Random Oracle Model

Readings: (highly recommended)

Katz/Lindell Chaps 1, 2, 3, 5

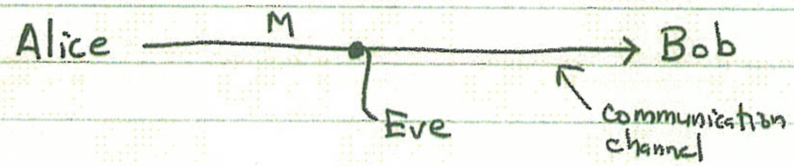
News:

- Anthem data breach (80M customers; $100M; govt employees)
- 100 banks/30 countries/$100M's or $1B? ATM's, etc. Carbanak ring
- PC spyware — rewriting disk firmware "Equation Group"
- Netgear wireless routers reveal admin password

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

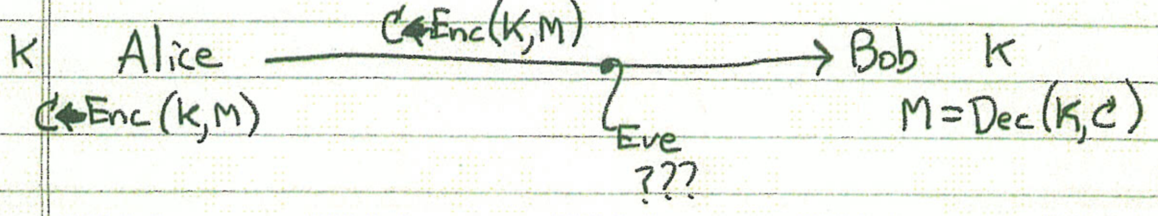
$M = Dec(K, C)$ decrypt C using K to obtain M

(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 } assumes K is re-used

chosen PT

chosen CT

...

{ Ciphertext indistinguishability

semantic security

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:**

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

- **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)

$$\begin{array}{lll} & M = 101100\cdots & (\lambda\text{-bit string}) \\ \text{Enc} \Downarrow & \oplus\ K = 011010\cdots & (\text{xor } \lambda\text{-bit "pad" (key)}) \\ \hline & C = 110110\cdots & (\lambda\text{-bit ciphertext}) \\ \text{Dec} \Downarrow & \oplus\ K = 011010\cdots & \\ \hline & M = 101100\cdots & \end{array}$$

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

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

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

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

Theorem: For OTP, $P(M) = P(M|C)$

$\cong$ "Eve learns nothing 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

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

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

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

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

$P(M|C)$ = 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 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 Venona!

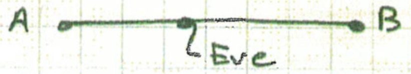
<u>Theorem:</u> OTP is <u>malleable</u>.

(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").

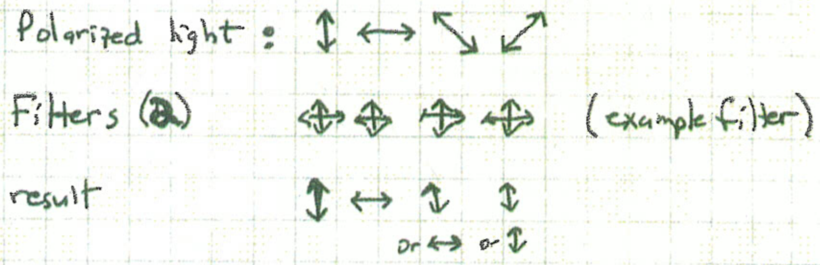
How to generate a random pad?

- Coins, cards
- Dice
- Radioactive sources (old memory chips were susceptible to alpha particles)
- Microphone, camera
- Hard disk speed variations
- Intel 82802 chip set now RdRand
- 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.

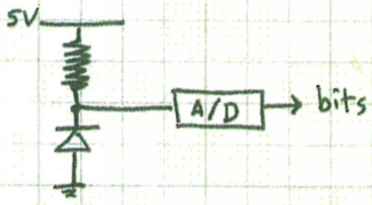
- Quantum Key Distribution



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

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

- "Noise diodes"



TOPIC:

DATE:

FILE UNDER:

PAGE: L4.6

Final project idea

smart phone app!

- generate pads using camera
- share pads when meet (a la "bump")
- send confidential messages