TOPIC: 6.857

DATE: 2/11/19

FILE UNDER:

PAGE L02.1

Admin: Pset #1 to be post this evening. (With groups)
Due 2/25

Today: Killian lecture ("Growth of Cryptography")

One-time pad (OTP)

Reading: Katz & Lindell, Chapter 2 (recommended)

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:

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

- 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)

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 ⇓

$\oplus\ K = 0\,1\,1\,0\,1\,0\,\cdots$

$M = 1\,0\,1\,1\,0\,0\,\cdots$

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

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)

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

Theorem: OTP is malleable.

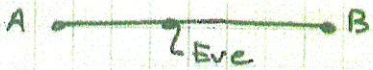
(That is, changing ciphertext bits causes corresponding bits of decrypted message to change.)

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

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

Polarized light: ↕ ↔ ↘ ↙

Filters (2) ✣ ✣ ✣ ✣ (example filter)

result ↕ ↔ ↕ ↕
or ↔ or ↕

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"