2/15/17
L3.1

Admin: Pset #1 posted, due 2/27

If needed, talk to TA's regarding groups.

- Watch Killian lecture by Prof. Rivest: "The Growth of Cryptography"

Today: - Enc

- One time Pad. (OTP)

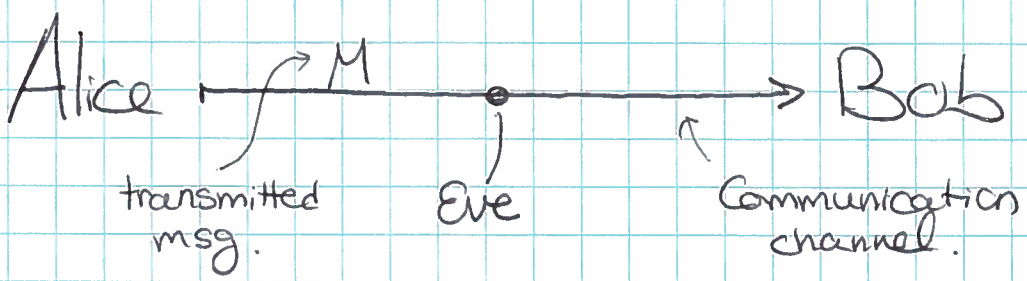
Reading: Katz-Lindell Chapters

Encryption:

Goal: Confidentiality of transmitted (or stored) msg.

Parties: Alice & Bob are "good guys"

Eve is "eavesdropper" / "adversary".



Eve can see all the msgs sent on the channel, but should not learn M.

In basic picture above there is nothing to distinguish Eve from Bob.

How do we ensure that Bob receives M, but Eve does not?

Crypto Approach

- Bob knows a key K that Eve doesn't (Eve knows the system,
- Alice can encrypt M so that knowledge of K allows for decryption.
- Eve sees ciphertext, but learns nothing about M.

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 is given to Gen in unary)

$C \leftarrow Enc(K, M)$: Encrypt msg M with key K. Result is C

$M = Dec(K, C)$: Decrypt C using K to obtain M.

Convention (Katz-Lindell):

"$\leftarrow$" for randomized computations
(often $\leftarrow_R$ or $\leftarrow_{\$}$ is used).

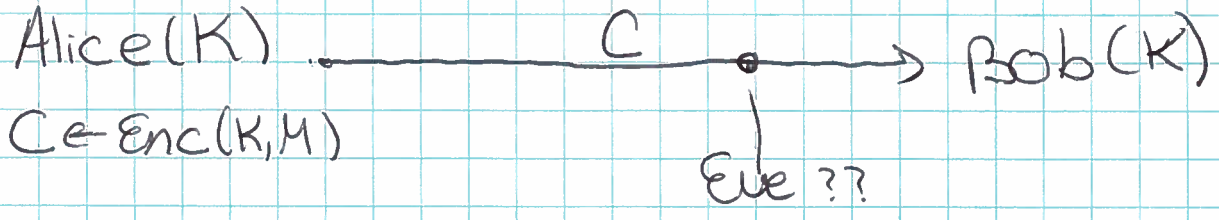
"$=$" for deterministic ones.

Why are Gen & Enc probabilistic? For security.

Why is Dec deterministic? Randomness is not needed for decryption.

Setup: Someone computes $K \leftarrow Gen(1^\lambda)$,
(may be Alice or Bob)

and ensures that Alice & Bob both have K
(and Eve doesn't). (How?!)



Security objectives:

Eve cannot distinguish $Enc(K, M_1)$ from $Enc(K, M_2)$
even if she knows (or chooses) M_1, M_2 (of same length).

[Encryption typically does not hide msg length]

This security notion is called "ciphertext indistinguishability" or "semantic security" [Goldwasser-Micali 82].

Attacks: - known ciphertexts
- known CT/PT pairs
- chosen PT
- chosen CT

} assumes K is reused.

Similar "game-based" def:

- Alice picks $K \leftarrow Gen(1^\lambda)$, and tells Eve λ (msg length).
- Eve chooses distinct M_0, M_1 of equal length λ.
- Alice chooses a random bit $b \leftarrow \{0,1\}$
- Alice gives $Enc(K, M_b)$ to Eve.
- Eve produces a guess $\hat{b}$ for b.
- Eve wins if $\hat{b} = b$

Eve's advantage is $Pr[\hat{b} = b] - 1/2$

Advantage should go to zero as $|K|$ increases.

Eg., "negligible" means goes to zero faster than $1/poly(|K|)$

One-Time Pad (OTP)

- Vernam 1917: Paper-tape based (patent).

[Proposed a teleprinter cipher in which a previously prepared key, kept on paper tape, is combined character by character w. plaintext msg to produce ciphertext]

- Msg, key, ciphertext have same length (λ bits)
- Key K also called pad. It is random & known only to Alice & Bob. (used by spies, key written on small pad...)

Enc:

$$M = 101100\ldots \quad \text{(binary string)}$$
$$\oplus\ K = 011010\ldots$$
$$C = 110110\ldots \quad \text{(mod 2 each column)}$$

Dec: Simply add K again:

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

Proved in WWII, published later

Thm [Shannon 49]: OTP is unconditionally secure (i.e., secure against Eve w. unlimited computational power) aka., information theoretically secure.

[as opposed to computational security, which assumes Eve is comp. bounded]

Proof: Let $P(M)$ = Eve's prior prob. that msg is M

$P(M|C)$ = Eve's posterior prob. that msg is M

Suffices to prove: $\forall C, M$

$P(M) = P(M|C) \Rightarrow$ "Eve learns nothing by seeing C"

Let $|M| = |K| = |C| = \lambda$

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

$\Rightarrow \forall C, M \quad P(C|M) =$ Prob C given M

$= \text{Prob } K = C \oplus M$

$= 2^{-\lambda}$

$\forall C \quad \Pr[C] =$ prob of seeing $\overbrace{C}^{\text{ciphertext}}$

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

$= \sum_M 2^{-\lambda} \cdot P(M) = 2^{-\lambda} \sum_M P(M) = 2^{-\lambda} \cdot 1 = 2^{-\lambda}$

($\to$ uniform)

$\Rightarrow P(M|C) =$ Prob of M after seeing C

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

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

$= P(M)$

QED

This is perfect security!

Negatives: Users need to:

- Generate large secrets
- Share them securely
- Keep them secret
- Avoid reusing them

} Usability ??

↳ $C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K) = M_1 \oplus M_2$

- Google "Venona Project" } Counter-intelligence program initiated by US Army's Signal Intelligence Service
Purpose: Dec of msgs transmitted by intelligence agencies of Soviet Union during the Cold War.

- Note: OTP is malleable

Namely, adv can change (eff.) ciphertext bits, causing the decrypted msg to change!

⇒ OTP does not provide any authentication of msg content or protection against modification ("mauling")