2/14/18
L3.1

Admin:
- Pset #1 posted, due Feb 26.
- Announcement: Daniel Genkin giving a talk at crypto day, Friday Feb 16, 2:45-3:45, G-882 on Spectre & Meltdown.

Today:
- Enc
- One time pad. (OTP)

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 <u>key</u> K that Eve doesn't
  (Eve knows the system, but not the key K).
- Alice can <u>encrypt</u> 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.
(K is shared symmetric key)

Algorithms:

$K \leftarrow Gen(1^\lambda)$: Generates key of length λ
(λ is given to Gen in unary, so we can say that Gen is a (probabilistic) poly time algorithm).

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

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

<u>Convention</u>:

"$\leftarrow$" for randomized computations

(often $\xleftarrow{R}$ or $\xleftarrow{\$}$ is used)

"$=$" for deterministic computations.

<u>Correctness Requirement</u>: $\forall M$

$$\Pr[\,\mathrm{Dec}(K, \mathrm{Enc}(K, M)) = M\,] = 1 - \mathrm{negl}(\lambda)$$

where the prob. is over $K \leftarrow \mathrm{Gen}(1^\lambda)$ and over the randomness of Enc & Dec.

$\mathrm{negl}(\lambda)$: A function that approaches 0 faster than $\frac{1}{\mathrm{poly}(\lambda)}$ (for every poly).

(Formally: $\mu(\lambda) = \mathrm{negl}(\lambda)$ if $\forall$ const. $c \in \mathbb{N}$ $\exists$ $N \in \mathbb{N}$ s.t. $\forall \lambda > N$ $\mu(\lambda) < \frac{1}{\lambda^c}$)

In crypto we are willing to tolerate negl error

* Why are Gen & Enc probabilistic? For security.

Why is Dec deterministic? Randomness is not needed for decryption

<u>Setup</u>: Someone computes $K \leftarrow Gen(1^\lambda)$
(may be Alice or Bob)

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

$$\text{Alice}(K) \xrightarrow{\quad C \quad} \text{Bob}(K)$$

$C \leftarrow Enc(K, M)$ Eve ??

<u>Security Definition</u>:

<u>Objective</u>: 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 "semantic security" [Goldwasser - Micali 82].
(also called "ciphertext indistinguishability").

<u>Formal Def</u>: $\forall$ Eve $\forall \lambda \in \mathbb{N}$ $\forall M_0, M_1$ ← of length λ adversarially chosen by Eve (given 1^λ)

$$\Pr[\, Eve(1^\lambda, Enc(K, M_b)) = b \,] = \frac{1}{2} + negl(\lambda)$$

This is known as a "<u>game-based</u>" definition

- Alice samples $K \leftarrow Gen(1^\lambda)$, and tells Eve (the 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 <u>advantage</u> is $Pr[\hat{b} = b] - 1/2$

Advantage should go to zero as λ increases (usually, we require advantage to be $negl(\lambda)$).

<u>Other security definitions</u>:

- known ciphertext attack
- known CT/PT pairs
- Chosen PT
- Chosen CT

} assumes K is reused.

One-Time Pad (OTP)

Invented by Gilbert Vernam 1917 : Paper-tape based (Patented).

Proposed a teleprinter cipher in which a previously prepared key, kept in paper tape (punched tape), is combined charachter-by-character w. plaintext msg to produce a ~~ct~~ ciphertext.

[patented for XOR operation]

- Msg, Key, ciphertext have same length (λ bits).
- Key K is called <u>pad</u>.

  It is random & known only to Alice & Bob

  (used by spies, key written on small pad)

<u>Enc</u>:

$$\begin{array}{rl} & M = 101100 \\ \oplus & K = 011010 \\ \hline & C = 110110 \end{array}$$

(mod 2 each column)

<u>Dec</u>: Simply XOR K again

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

Thm [Shannon 49]: OTP is unconditionally secure

proved in WWII, published later.

(i.e., secure against Eve w. unlimited computational power)

a.k.a. information theoretically secure.

[As opposed to computational security, which assumes Eve is computationally bounded]

Proof: Recall (by def) Eve chooses M_0, M_1 of length λ, & a bit $b \leftarrow \{0,1\}$ is chosen at random.

Let $Pr[C]$ = prob that the encryption that Eve receives is C.

$Pr[C|b]$ = Prob that Eve receives ciphertext C conditioned on b being the chosen bit. (i.e. Eve receives enc. of M_b)

Similarly: $Pr[b]$, $Pr[b|C]$

We ~~[illegible]~~ prove $\forall b \in \{0,1\}$ $\forall C$

$$Pr[b|C] = \frac{1}{2}. \quad \longleftarrow \text{Perfect security!}$$

$$Pr[b|C] = \frac{Pr[C|b] \cdot Pr[b]}{Pr[C]} = \frac{Pr[C|b]}{Pr[C]} \cdot \frac{1}{2}$$

Bayes' Rule.

Need to prove

$$\Pr[C] = \Pr[C \mid b]$$

We will prove that they both equal $\frac{1}{2^\lambda}$:

$$\Pr[\underset{\substack{\parallel \\ K \oplus M_b}}{C} \mid b] = \Pr[K = C \oplus M_b] = \frac{1}{2^\lambda}$$

$$\Pr[C] = \Pr[C \mid b=0] \cdot \Pr[b=0] + \Pr[C \mid b=1] \cdot \Pr[b=1]$$

$$= \frac{1}{2^\lambda} \cdot \frac{1}{2} + \frac{1}{2^\lambda} \cdot \frac{1}{2} = \frac{1}{2^\lambda} \qquad \blacksquare$$

This is perfect security!

<u>Negatives</u>:

- Generate large keys
- Share them securely
- Keep them secret
- <u>Avoid reusing them</u>!

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

* Google "Venona Project"

Counter-intelligence program initiated by US Army signal intelligence service.

<u>Purpose</u>: Dec of msgs transmitted by intelligence agencies of Soviet Union during Cold War

<u>Note</u>: OTP is <u>malleable</u>

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

$\Rightarrow$ OTP does not provide any authentication of msg or content, or protection against modification ("mauling").