Special Topics in Cryptography

Mohammad Mahmoody

Problem set 1

- Will posted today
- You have till Thursday (1Feb) 6pm to submit it on Collab.

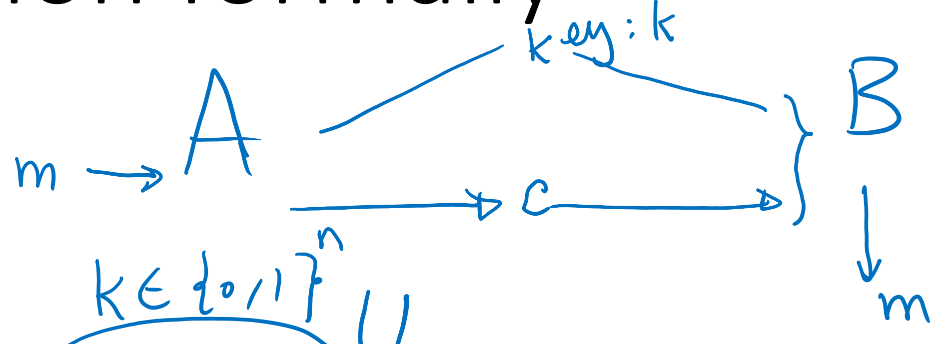
Last time

- A bird's eye view of the topics
- The Kerckhoffs's principle
- Caesar and Jefferson ciphers

Today

- Defining encryption formally (secret key) symmetric-key
- Information theoretic (perfect) vs. computational secrecy

Defining secret-key encryption formally



Encryption Scheme:

3 Algorithms

① key generation $\quad G(\overbrace{\text{key length}}^{n}) \longrightarrow \text{key}\ (k)$ $\quad k \in \{0,1\}^n \quad U_n$

② Encryption : $\quad Enc(k, m) = c \in \mathcal{C}$

plaintext. $m \in \mathcal{M}$

③ Decryption $\quad Dec(k, c) = m \in \mathcal{M}$

$k \in \mathcal{K}$

$m \in \mathcal{M}$

$c \in \mathcal{C}$

$\forall_{k \in \mathcal{K}, m \in \mathcal{M}}$: ① $Enc(k, m) = c$ ② $Dec(k, c) = m'$ $\Longrightarrow m = m'$:

Completeness Condition.

The setting

- Encryption happens just once (but maybe for a very long message).
- Enc and Dec both just take the secret key (no extra randomness)

- (We will use a more general definition later on..)

Defining Perfect Secrecy 1st try (semantic secrecy)

- Idea: the ciphertext does not change what Eve knew about plaintext.

$$\begin{tikzcd} m & A \arrow[r] & c \arrow[r] & B \\ & & E \arrow[u, dotted] & \end{tikzcd}$$

If Eve has some "uncertainty" about m: it should not change after seeing ciphertext $\underline{c}$.

Probability (Basics)

Mapping $P(\cdot)$

- Distributions and random variables

for every (Ω, P) a random variable V is a variable that if we sample from ($v \leftarrow V$) we get something from Ω according to P

Set Ω: $\{a_1, a_2, \ldots, a_m\}$

$P_i = \Pr[a_i]$: probability of selecting a_i $\quad P_i \in [0,1]$

$$\sum_i P_i = 1$$

$$\underbrace{(\Omega, P(\cdot))}_{\text{prob. space.}}$$

$P(i) = P(a_i) = P_i$

example: Pick a random number in $\underbrace{\{0, \ldots, 20\}}_{\Omega}$ $\quad \Pr_{i \in \Omega}[i] = 1/21$

example 2: key $\in \underbrace{\{0,1\}^{100}}_{\Omega}$ $\quad \Pr_{x \in \Omega}[x] = \frac{1}{2^{100}}$

Event: $E \subseteq \Omega$

$$\Pr[E] = \sum_{i \in E} P_i$$

example. $E: \{0, 2, 4, \ldots, 20\} \subseteq \{0, \ldots, 20\}$

$$\Pr[E] = \sum_{i \in E} P_i = 11 \times \frac{1}{21} = \frac{11}{21}$$

Probability (Basics)

$P(\text{rainy}, \text{NoTr}) = 0$

$\{\text{sunny}, \text{rainy}, \text{cloudy}\}$

$\{\text{NoTraffic}, \text{Some-Traffic}\}$

- ~~Conditional distributions~~, and independent random variables

$\Omega = (\Omega_1 \times \Omega_2) = \{ \underbrace{(a,b)}_{c} \mid a \in \Omega_1, b \in \Omega_2 \}$

let $\underline{P}$ is a dist over Ω : $P((a,b)) \to [0,1]$

if $\forall (a,b) \in \Omega$
$P[(a,b)] = P_1[a] \cdot P_2[b]$

$\to$ We call P_1 & P_2 independent

"knowing a does not chang the chance of b"

$P_1(a) = ?$ if we pick $(a', b') \leftarrow P$ (as a random variable)

what is the chance of getting $a = a'$?

$a \in \Omega_1$

$\sum_{b \in \Omega_2} P(a,b)$: P_1 prob. dist over Ω_1

think about sampling a from Ω_1 and b from Ω_2 independently.

$G \longrightarrow \boxed{k \in \mathcal{K}}$ uniform.

Suppose m is distributed according to $\boxed{M}$

② $Enc(k, m) \longrightarrow c$ ③ $Dec(c, k) \longrightarrow m$.

Let C be the distribution of ciphertex c

Let ~~M~~ K be the random variable for uniform key $\underline{\underline{k}} \longleftarrow K$

3 random variables $\underline{(K, M, C)}$

$\underline{C}$ is NOT independent of $\underbrace{(K, M)}_{X}$

Def: Perfect Secrecy: M and C are independent random Variable.

Shannon's defenition of secrecy.

$C_1 = k \oplus m_1$ $C_2 = k \oplus m_2$ | $C_1 \oplus C_2 = m_1 \oplus m_2$

A scheme with perfect semantic security

- One Time Pad (OTP) scheme:

$m \in \{0,1\}^n = \mathcal{M}$ $|m| = |k|$

$k \in \{0,1\}^n = \mathcal{K}$

Bob has a random key $k \in \{0,1\}^n$

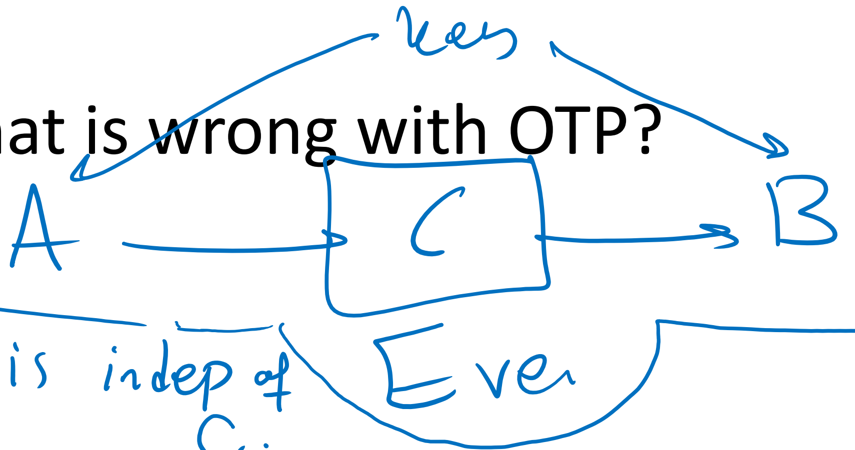
$\mathrm{OTPEnc}(m, k) \xrightarrow{?} c$ such that c becomes completely independent of message m.

$c \overset{Enc}{=} m \oplus k$: bit by bit XOR.

$\mathrm{Dec}(c, k) \xrightarrow{?} m$

$c \oplus k = (m \oplus k) \oplus k = m$

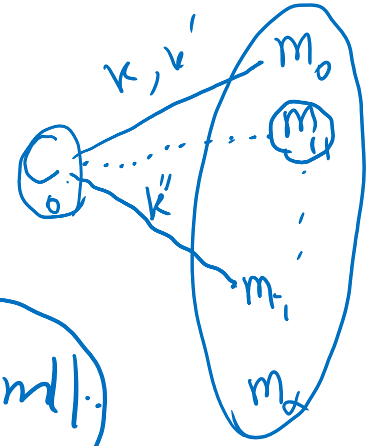
- What is wrong with OTP?



Thm: M is indep of C.

Shannon's theorem:
Perfect semantic secrecy requires "long" keys

Thm: if we encrypt only one $m \in \mathcal{M}$ using a key $k \in \mathcal{K}$. then achieving perfect secrecy is Impossible if ~~[illegible]~~ $|k| < |m|$.



Proof:

Lemma: if $\exists\, m_0, C_0$: ciphertext that c_0 cannot be decrypted into plaintext m_0 no matter what key k used.. $\longrightarrow$? $\Rightarrow$ the schem is NOT perfectly secret.

If perfect secrecy $\longrightarrow \forall\, c_0, m_0\ \exists\, k_0\ \ \mathrm{Dec}(c_0, k_0) = m_0$

$c_0 \xrightarrow{\exists k\ \mathrm{Dec}(c_0,k)} m_0, m_1, \ldots \quad \mathcal{M}$

Defining Perfect Secrecy, 2^{nd} try (perfect indistinguishability)

- Idea: Eve cannot guess the message, even if she knows $m \in \{m_0, m_1\}$

$\forall m_0, m_1$

Security Game:

$m_0, m_1 \in \mathcal{M}$

Challenger

Adv.

m_0, m_1

Pick $b \in \{0,1\}$

Pick key $k \in \{0,1\}^n$

get: $C = Enc(m_b, k)$

c

b' :

Adv wins if $b = b'$

Def: for all ADV

$\Pr[\text{ADV win}] \le \frac{1}{2} \ldots$

Perfect semantic secrecy and perfect indistinguishability… are equivalent!

Problem: So again we need keys as long as messages!

Relaxing perfect indistinguishability : (statistical indistinguishability)

$\varepsilon = 2^{-100}$

- Idea: Eve **cannot guess** the message with probability $\frac{1+\varepsilon}{2}$ even if she knows $m \in \{m_0, m_1\}$

Sec Gam

Def: $\forall$ Adv

$\Pr[\mathrm{Win}] \leq \frac{1+\varepsilon}{2}$

Challenger $\xleftarrow{m_0,\ m_1}$ Adv

$b \in \{0,1\}$

$k \in \{0,1\}^n$

$\xrightarrow{c}$

$\xleftarrow{b'}$

Wins if

$b = b'$

Shannon's theorem:
Statistical indistinguishability ..still needs "long" keys!

even $\varepsilon = \frac{1}{2} \longrightarrow \Pr[\mathrm{Win}] = \frac{1+\frac{1}{2}}{2} = \frac{3}{4}$

it still implies $|\mathrm{key}| \geq \frac{|m|}{2}$

just an extension of previous proofs

Computational Secrecy

How to rely on computational complexity?

We are OK if Adv can break the scheme in 2^{1000} steps!