Quiz 1 : 10% ; MidSem : 15% ; Quiz 2 : 10% ;
EndSem : 30% ; Project : 30% ; Scribe : 5%

Scribe : One team per lecture until midsem
then 2 per lecture

Project : 5 per team (100 marks),
Proposal : 10, Lit Survey : 15, Problem formulation
: 15, Soln. proposal : 30, Presentation : 30

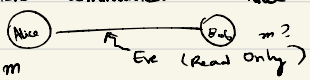
Make - Break - Patch cycle → more art than science

Shannon - Made it a science - Can we define unbreakable cipher?

Perfect Secrecy -

Setup :

Consider communication channel :



Instead of transmitting m, transmit c such that $c \leftarrow Enc(m)$ where acc. to Kirckhoff principle, Encoding fn. is public. Only intended recipient should be able to transform $c \to m$, but if recipient is as yet undecided, All are eavesdroppers.

Assume key K is known by both Alice & Bob.
If key K is null, it is same old method.
(This scheme considers only same key b/w Alice & Bob). Instead use $c \leftarrow Enc_K(m)$ & $m' \leftarrow Dec_K(c)$. Correctness is $m = m'$. m is chosen from message space $\mathbb{M}$ ($m \in \mathbb{M}$). $k \in$ keyspace $\mathbb{K}$. $Enc : \mathbb{M} \times \mathbb{K} \to \mathbb{C}$ (ciphertspace)
$Dec : \mathbb{C} \times \mathbb{K} \to \mathbb{M}$. Gen assigns keys to Alice & Bob.
(Gen : key generator)

$Gen : \frac{len\ of}{Key} \to \mathbb{K}$ (equivalently, $1^n \to \mathbb{K}$)

Encryption scheme is a 4 tuple of
$\langle \mathbb{M}, Gen, Enc, Dec \rangle$ (Fixing Dec & Enc $\mathbb{C}$, Gen fixes $\mathbb{K}$)
Every historic enc. scheme can be expressed in this form.

Defn : An encryption scheme $\langle \mathbb{M}, Gen, Enc, Dec \rangle$ is perfectly secure if $\forall$ probability distributions over $\mathbb{M}$, $\forall\ m \in \mathbb{M}$, $\forall\ c \in \mathbb{C}$,

D1 $P[Message = m \mid Ciphertext = c] = P[Message = m]$
where $P[Ciphertext = c] \neq 0$

Consider message space $\mathbb{M}$. $\mathbb{M}$ can be modelled as a random variable where m is an event in $\mathbb{M}$. The information contained in $\mathbb{M}$ is the avg. no. of bits needed to simulate the pdf of $\mathbb{M}$ over infinite trials

Ex : Instead of storing probability p, store $1/p$. The number of bits to be used is $\log_2(1/p)$

$E[\#\text{bits}] = \sum_i p_i \log_2(1/p_i)$

---

which implies $H(\mathbb{M}|\mathbb{C}) = H(\mathbb{M})$
(but H equal does not imply P equal)

Vernam Cipher (One - Time Pad)

$\mathbb{M} = \{0,1\}^n$, $\mathbb{K} = \{0,1\}^n$, $\mathbb{C} = \{0,1\}^n$

$Gen(1^n) : k \in_R \{0,1\}^n$
↳ uniformly at random

$Enc_K(m) = m \oplus k$ (Bitwise xor)
$Dec_K(c) = c \oplus k$

Key is used only once, so called one time pad.

The defn. of perfect secrecy $\Leftrightarrow$ $\forall$ prob. dist $\mathbb{M}$,

D2 $\forall\ m \in \mathbb{M}$, $\forall\ c \in \mathbb{C}$, $P[\mathbb{C}=c \mid \mathbb{M}=m] = P[\mathbb{C}=c]$

by Bayes Theorem

$$P[A \mid B] = \frac{P[B \mid A]\ P[A]}{P[B]}$$

Equivalently, $\forall\ m_0, m_1 \in \mathbb{M}$, $\forall$ pr. dist $\mathbb{M}$, $\forall\ c \in \mathbb{C}$

$P[\text{Ciphertext}=c \mid \text{Message}=m_0] = P[\text{ciphertext}=c \mid \text{Message}=m_1]$

(By substituting $m=m_0$ & $m=m_1$ in defn. 2,

D3 $P[\mathbb{C}=c \mid \mathbb{M}=m_0] = P[\mathbb{C}=c] = P[\mathbb{C}=c \mid \mathbb{M}=m_1]$)

$$P[C=c] = \sum_{m \in \mathbb{M}} P(M=m) \cdot P[C=c \mid M=m]$$

$$= P[C=c \mid M=m] \sum_{m \in \mathbb{M}} P(M=m)$$

by defn. 3 & transitiveness

$$P[C=c) = P[C=c \mid M=m)$$

To show perfect secrecy, show that it satisfies definition 3.

In Vernam cipher, $P[C=c \mid M=m_0]$

$= P[K = m_0 \oplus c] = 1/2^n$ since key is randomly chosen at uniform.

Similarly for m_1.

When sender & receiver are same, there is no need for secure comm. of key & Vernam cipher is unbreakable