

$\text{Gen} : \{0,1\}^n \xrightarrow{\text{KCH}} \mathcal{K}$ (equivalently, $1^n \rightarrow \mathcal{K}$)

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 \rightarrow more art than science

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

Encryption scheme is a 4 tuple of

$\langle M, \text{Gen}, \text{Enc}, \text{Dec} \rangle$ (Fixing Dec & Enc
 C , Gen fixes \mathcal{K})

Every historic enc. scheme can be expressed
in this form.

Defn: An encryption scheme $\langle M, \text{Gen}, \text{Enc}, \text{Dec} \rangle$

is perfectly secure if \forall probability distributions
over M , $\forall m \in M$, $\forall c \in C$,

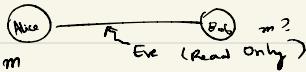
$$D1: p[\text{Message} = m \mid \text{Ciphertext} = c] = P[\text{Message} = m]$$

where $p[\text{Ciphertext} = c] \neq 0$

Perfect Secrecy -

Setup:

Consider communication channel:



Instead of transmitting m , transmit c such that
 $c \leftarrow \text{Enc}(m)$ where acc. to Kerckhoff principle,
Encoding fn. is public. Only intended recipient
should be able to transform $c \rightarrow m$, 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 $c \leftarrow \text{Enc}_K(m)$ &
 $m' \leftarrow \text{Dec}_K(c)$. Correctness is $m = m'$. m

is drawn from message space $M (m \in M)$. K is

keyspace \mathcal{K} . Enc: $M \times \mathcal{K} \rightarrow C$ (Ciphertext space)

Dec: $C \times \mathcal{K} \rightarrow M$. Gen assigns keys to
Alice & Bob.
Key generator

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

Eg: instead of storing probability p , store
 γ_p . The number of bits to be used is $\log(\frac{1}{p})$
 $E[\# \text{bits}] = \sum p_i \log_2(\frac{1}{p_i})$

which implies $H(M|c) = H(M)$

(but H equal does not imply p equal)

Vernam Cipher (One-Time Pad)

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

$$\text{Gen}(1^n) : k \in_R \{0,1\}^n$$

uniformly at random

$$\text{Enc}_K(m) = m \oplus k \quad (\text{Bitwise } \oplus \text{or } \text{XOR})$$

$$\text{Dec}_K(c) = c \oplus k$$

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

The defn. of perfect secrecy \Leftrightarrow if prob. dist. M ,
 $D \in \{m \in M\}$, & $c \in C$, $P[C=c|M=m] = P[C=c]$

by Bayes Theorem.

$$P[A|B] = \frac{P[B|A] \cdot P[A]}{P[B]}$$

Equivalently, if $m_0, m, \in M$, if pr. dist. M , $C \in C$

$$P[C=c|M=c_0] = P[C=c|M=m]$$

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

$$D^3 \quad P[C=c|M=m_0] = P[C=c] = P[C=c|M=m_1]$$

$$\begin{aligned} P[C=c] &= \sum_{m \in M} P(M=m) \cdot P[C=c|M=m] \\ &= P[C=c|M=m] \sum_{m \in M} P(M=m) \end{aligned}$$

by defn. 3
& transitivity

$$P[C=c] = P[C=c|M=m]$$

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

$$\begin{aligned} \text{In Vernam cipher, } P[C=c|M=m_0] \\ &= P[K=m_0 \oplus c] = \frac{1}{2^n} \text{ since key} \\ &\text{is randomly chosen at uniform.} \end{aligned}$$

Similarly for m_1 .

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