UNIT-2 :-

Shannon's Theory :-

- Discrete Random Variable.
- Probability distribution.
- Joint Probability.
- Conditional Probability.
- Baye's Theorem.

→ Crypto system ⇒ $(P, C, K, \mathcal{E}, D)$. ⇒ $\boxed{D_K(E_K(x)) = x}$

→ A particular key $k \in K$ is used for one encryption.

Probabilities :-

⇒ $P(X = x)$ → Plaintext random variable.

$P(K = k)$ → Key " "

$P(Y = y)$ → Ciphertext " ".

Independent Random variable :-

X & Y independent R.V iff $P(x/y) = P(x)$

$\forall\, x \in X, y \in Y$.

→ Both plaintext (x) and key (K) are chosen independently. So, they are independent random variables.

⇒ Ciphertext set,

$$C(K) = \{E_K(x) ; x \in P\}.$$

Q) $P = \{a, b\}$. $K = \{K_1, K_2, K_3\}$.

$P(a) = 1/4$ $P(K_1) = 1/2$

$P(b) = 3/4$ $P(K_2) = 1/4$

$P(K_3) = 1/4$

$C = \{1, 2, 3, 4\}$.

$E_K(x)$	a	b
K1	1	2
K2	2	3
K3	3	4

Sol: Need to find 'y' probabilities first. ($\because$ since we already know x & K probabilities)

$$P(Y=y) = \sum_{K: y \in C(K)} P(K=k) \cdot P(x = D_K(y))$$

$$\cancel{= P(K=K_1) \cdot P(x=a) + P(K=K_2) \cdot P(x=a)}.$$

$$C(K) = \{E_K(x) ; x \in P\}.$$

$$C(K_1) = \{E_{K_1}(x) ; x \in P\}.$$

$$= \{E_{K_1}(a), E_{K_1}(b)\}.$$

$$\Rightarrow C(K_1) = \{1, 2\}.$$

$$C(K_2) = \{2, 3\} \quad C(K_3) = \{3, 4\}.$$

$$\Rightarrow P(Y=1) = \sum_{\{K : 1 \in C(K)\}} P(K=K) \cdot P(X = D_K(1)).$$

$$= P(K=K_1) \cdot P(X = D_{K_1}(1)).$$

$$= P(K=K_1) \cdot P(x=a).$$

$$= 1/2 \times 1/4$$

$$\therefore P(Y=1) = 1/8$$

$$P(Y=2) = \sum_{\{K : 2 \in C(K)\}} P(K=K) \cdot P(X = D_K(2)).$$

$$= P(K=K_1) \cdot P(X = D_{K_1}(2)) + P(K=K_2) \cdot P(X = D_{K_2}(2))$$

$$= P(K=K_1) \cdot P(X=b) + P(K=K_2) \cdot P(X=a).$$

$$= 1/2 \times 3/4 + 1/4 \times 1/4.$$

$$= \frac{3\times2}{8\times2} + \frac{1}{16} = \frac{7}{16}.$$

$$P(Y=3) = \sum_{\{K:3\in C(K)\}} P(K=k) \cdot P(X=D_K(3))$$

$$= P(K=k_2)\cdot P(X=D_{K_2}(3)) + P(K=k_3)P(X=D_{K_3}(3))$$

$$= P(K=k_2)\cdot P(X=b) + P(K=k_3)\cdot P(X=a)$$

$$= \frac{1}{4}\times 3/4 + 1/4 \times 1/4$$

$$= \frac{4}{16} = \frac{1}{4}$$

$$P(Y=4) = \sum_{\{K:4\in C(K)\}} P(K=k)\cdot P(X=D_K(4))$$

$$= P(K=k_3)\cdot P(X=D_{K_3}(4))$$

$$= P(K=k_3)\cdot P(X=b)$$

$$= 1/4 \times 3/4 = 3/16$$

$$P(Y) = P(Y=1) + P(Y=2) + P(Y=3) + P(Y=4)$$

$$= 1/8 + 7/16 + \frac{1\times 2}{4\times 2} + 3/16$$

$$= \frac{3\times 2}{8\times 2} + \frac{10}{16} = \frac{16}{16} = 1$$

$P(Y=1/x=a) = ?$

$P(y=1/x=b) = ?$

$$P\left(\frac{y=1}{x=a}\right) = \frac{P((y=1)\cap(x=a))}{P(x=a)}.$$

$= ??$

* **Modular Exponentiation :-**

Eg :- $88^7 \bmod 187$.

$88^1 \bmod 187 = 88$.

$88^2 \bmod 187 = 88 \times 88 \bmod 187$

$= 7744 \bmod 187$

$= 77$

$88^4 \bmod 187 = 88^2 \times 88^2 \bmod 187$

$= 77 \times 77 \bmod 187$

$= 5929 \bmod 187$

$= 132$.

$88^7 \bmod 187 = 88^4 \times 88^2 \times 88^1 \bmod 187$

$= 132 \times 77 \times 88 \bmod 187$

$= 894.432 \bmod 187$

$= 11$

Eg :- last two digits of 29^5

$29^5 \bmod 100 = ?$

$29^1 \bmod 100 = 29$

$29^2 \bmod 100 = 841 \bmod 100$,

$= 41$

$29^4 \bmod 100 = 29^2 \times 29^2 \bmod 100$

$= 41 \times 41 \bmod 100$

$= 1681 \bmod 100$

$= 81$

$29^5 \bmod 100 = 29^4 \times 29^1 \bmod 100 = 81 \times 29 \text{ m}$

$= 2349 \bmod 10$

Eg:- $3^{100} \bmod 29$

$3^1 \bmod 29 = 3 \bmod 29$

$3^2 \bmod 29 = 9 \bmod 29$

$3^4 \bmod 29 = 81 \bmod 29.$

$= 23 \bmod 29 = -6 \bmod 29$

$3^8 \bmod 29 = 3^4 \times 3^4 \bmod 29$

$= -6 \times -6 \bmod 29$

$= 36 \bmod 29$

$= 7 \bmod 29.$

$3^{16} \bmod 29 = 3^8 \times 3^8 \bmod 29$

$= 7 \times 7 \bmod 29$

$= -9 \bmod 29.$

$3^{32} \bmod 29 = 3^{16} \times 3^{16} \bmod 29$

$= 81 \bmod 29$

$= -6 \bmod 29$

$3^{64} \bmod 29 = 3^{32} \times 3^{32} \bmod 29$

$= 36 \bmod 29,$

$= 7 \bmod 29.$

$3^{100} \bmod 29 = 3^{64} \times 3^{32} \times 3^4 \bmod 29$

$= 7 \times -6 \times -6 \bmod 29.$

$= 36 \times 7 \bmod 29$

$= 252 \bmod 29$

$= 20 \bmod 29$

⊛ Perfect Secrecy :-

A cryptosystem has perfect secrecy if.
$P(x/y) = P(x) \quad \forall\, x \in P \;\&\; y \in C$.

⊛ Theorem :-

Suppose the 26 keys in the shift cipher are used with equal probability $1/26$. Then for any plaintext probability distribution, the shift cipher has perfect secrecy.

Pf :-

$$P = C = K = \mathbb{Z}_{26}.$$

$$y = E_K(x) = x + K \pmod{26}$$

$$x = D_K(y) = y - K \pmod{26}.$$

$$\forall\, x \in P,\; y \in C,\; K \in K.$$

Given, $P(K=k) = \frac{1}{26}$.

We have to prove, $P(x/y) = P(x)$. $\forall x \in P,\ \forall y \in C$.

We know that, $P(x/y) = \dfrac{P(X=x) \cdot P(Y=y/X=x)}{P(Y=y)}$.

$$P(Y=y/X=x) = \sum_{\{K : x = D_K(y)\}} P(K=K).$$

$$P(Y=y) = \sum_{\{K : y \in C(K)\}} P(K=K) \cdot P(X = D_K(y)).$$

$$P(Y=y/X=x) = \frac{1}{n}\left(\sum 1\right)$$

$$= \frac{1}{n} = \frac{1}{26}$$

From $P(K=k) = \frac{1}{26}$.

$$P(Y=y) = \frac{1}{26} \sum_{K : y \in C(K)} P(x = D_K(y)).$$

$$P(Y=y) = \frac{1}{26} \sum_{K \in Z_{26}} P(X = D_K(y)).$$

$C(K) = Z_{26}$

	a	b	...	z
K=0	a	b	...	z
K=1	b	c	...	a

$$= \frac{1}{26} \times \sum_{x \in Z_{26}} P(X=x).$$

$$= \frac{1}{26}(1)$$

Sum of all probabilities.

$$= \frac{1}{I}$$

$$\therefore \; P(X/Y) = \frac{P(X=x) \cdot 1/26}{1/26}.$$

$$P(X/Y) = P(X=x), \quad \forall x \in P, \; \forall y \in C.$$

Ex:- Latin Square.

Let 'n' be a +ve integer. A latin square of order 'n' is an $n \times n$ array 'L' of the integers 1, 2, ---- n. such that every one of the 'n' integers occurs exactly once in each row and each column of 'L'.

Ex:- $n = 3$, order = 3.

1	2	3
3	1	2
2	3	1

Given, any Latin square be of order 'n', we can define a related crypto system.

Take $P = C = K = \{1, 2, ----, n\}$.

For $1 \leq i \leq n$, the encryption (given) ~~cryptosystem~~ defined as

$$E_i(j) = L(i,j).$$

Claim :- The Latin ~~system~~ square cryptosystem achieves Perfect secrecy provided that every key used with equal probability.

Ex ① :-

Given, encryption rule

	a	b	c	d
K_1	1	2	4	3
K_2	2	1	3	4
K_3	2	3	1	4

$P(K_1) = 1/2$, $P(K_2) = P(K_3) = \frac{1}{4}$

$P(a) = \frac{1}{4}$, $P(b) = \frac{1}{4}$

$P(c) = \frac{1}{4}$, $P(d) = \frac{1}{4}$

What $P(a/x) = ?$

$P(a/y) = ?$

Whether the system has perfect Secrecy?

Soln

(*) Prove that affine cipher achieves perfect secrecy if every key is used with equal prob. $1/312$.

(*) Entropy :-

→ Toss a coin ⇒ $\{T, H\}$ [∵ How much information is uncertain].

→ Measure in terms of bits $\{0, 1\}$.

→ Toss coin 'n' times ⇒ uncertain bits is 'n' bits.

$$\boxed{E = -\log_2 A}$$

$$E = -\log_2 \frac{1}{2^n}$$

$$= n . \log_2 2 = n \text{ (entropy)}.$$

(*) **Def**:-

Suppose 'X' is ~~distributed~~ discrete R.V. which takes on values from finite set, then the entropy of the R.V. 'X' is defined as,

$$H(X) = -\sum_{x \in X} P(x) \cdot \log_2 P(x).$$

Remark:- $y = 0$, $\log_2 0 = ?$

$$\boxed{\lim_{y \to 0} \log_2 y = 0}$$

Note:- If $|X| = n$, $P(x) = \frac{1}{n}$, $\forall x$.

Then,

(1) $H(X) = \log_2 n$.

(2) $H(X) \geq 0$.

(3) $H(x) = 0$ iff $P(x_0) = 1$ for some $x_0 \in X$.

$P(x_0) = 0 \ \forall x \neq x_0$.

Q) $P = \{a, b\}$, $P(a) = \frac{1}{4}$, $P(b) = \frac{3}{4}$,

$K = \{K_1, K_2, K_3\}$. $P(K_1) = \frac{1}{2}$, $P(K_2) = P(K_3) = \frac{1}{4}$.

$C = \{1, 2, 3\}$.

	a	b
K1	1	2
K2	2	3
K3	3	4

Find:

$H(P) = ?$

$H(K) = ?$

$H(C) = ?$

Sol:

$$H(x) = -\sum_{x} P(x) \cdot \log_2 P(x).$$

$$H(P) = -\left(P(a) \cdot \log_2 P(a) + P(b) \log_2 P(b)\right).$$

$$= -\frac{1}{4}\log_2\frac{1}{4} - \frac{3}{4}\log_2\frac{3}{4}$$

$$= \frac{1}{2} + \frac{3}{4}\times 0.41 = 0.81.$$

$$H(K) = -\left(P(K_1).\log_2 P(K_1) + P(K_2).\log_2 P(K_2) + P(K_3).\log_2 P(K_3)\right)$$

$$= 1.5$$

$$H(C) = -\left(P(1).\log_2 P(1) + P(2).\log_2 P(2) + P(3)\log_2 P(3) + P(4).\log_2(P(4))\right).$$

$$P(Y=y) = \sum_{\{K: y \in C(K)\}} P(K).\,P(X = D_K(y)).$$

$$P(y=1) = P(K_1).\,P(X=a).$$

$$= \frac{1}{2}\times\frac{1}{4} = \frac{1}{8}.$$

$$P(y=2) = P(K_1).\,P(x=b) + P(K_2).\,P(x=a).$$

$$= \frac{\cancel{2}}{2\times 2}\times\frac{3}{4} + \frac{1}{4}\times\frac{1}{4}$$

$$= \frac{7}{16}.$$

$$P(y=3) = P(K_2).\,P(x=b) + P(K_3).\,P(x=a).$$

$$= \frac{1}{4}\times\frac{3}{4} + \frac{1}{4}\times\frac{1}{4} = \frac{4}{16} = \frac{1}{4}$$

$$P(y=4) = P(K_3).\,P(x=b).$$

$$= \frac{1}{4}\times\frac{3}{4} = \frac{3}{16}.$$

$$\Rightarrow H(C) = -\left(\frac{1}{8}\log_2\frac{1}{8} + \frac{7}{16}\log_2\frac{7}{16} + \frac{1}{4}\log_2\frac{1}{4} + \frac{3}{16}\log_2\frac{3}{16}\right)$$

$$= 1.86.$$

Q).

E_K	a	b	c
K1	1	2	3
K2	2	3	4
K3	3	4	1

$P(K_1) = P(K_2) = P(K_3) = \frac{1}{3}$

$P(a) = \frac{1}{2}$, $P(b) = \frac{1}{3}$,

$P(c) = \frac{1}{6}$.

Find $H(c)$.

Sol

$$P(1) = P(K_1).P(a) + P(K_3).P(c)$$

$$= \frac{1}{3} \times \frac{\cancel{1}3}{2\times 3} + \frac{1}{3} \times \frac{1}{6}$$

$$= \frac{\cancel{4}2}{\cancel{18}9} = \frac{2}{9}$$

$$P(2) = P(K_2).P(a) + P(K_1).P(b)$$

$$= \frac{1}{3} \times \frac{1}{2} + \frac{1}{3} \times \frac{1}{3}$$

$$= \frac{1}{6} + \frac{1}{9} = \frac{\cancel{15}5}{\cancel{54}18} = \frac{5}{18}$$

$$P(3) = P(K_3).P(a) + P(K_2).P(b) + P(K_1).P(c)$$

$$= \frac{1}{3} \times \frac{1}{2} + \frac{1}{3} \times \frac{1}{3} + \frac{1}{3} \times \frac{1}{6}$$

$$= \frac{1}{3}\left(\frac{1\times 3}{2\times 3} + \frac{1\times 2}{3\times 2} + \frac{1}{6}\right)$$

$$= \frac{\cancel{6}}{3\times\cancel{6}} = \frac{1}{3}$$

$$P(4) = P(K_3).P(b) + P(K_2).P(c)$$

$$= \frac{1}{3} \times \frac{1\times 2}{3\times 2} + \frac{1}{3} \times \frac{1}{6}$$

$$= \frac{\cancel{3}1}{\cancel{18}6} = \frac{1}{6}$$

$$H(c) = -\sum_{i=1}^{4} P(y=i)\log_2 P(y=i)$$

(*) Suppose (P, K, C, E, D) is a cryptosystem.

Given a key $K \in K$, there exists only one $x \in P$ with condition $x = D_K(y)$ for any $y \in C(K)$.

Pf :-

Suppose there are $x_0 \neq x_1$ in P such that

$$x_0 = D_K(y).$$

$$x_1 = D_K(y) \quad \text{for same } y \in C(K).$$

$$\longrightarrow y = E_K(x_0),\ y = E_K(x_1)$$

$$x_0 = D_K(E_K(x_0))$$

$$= D_K(y).$$

$$= D_K(E_K(x_1)).$$

$$\therefore x_0 = x_1$$

This is a contradiction.

(*) Jensen's inequality :-

- Jensen's inequality.
- $H(X,Y) \leq H(X) + H(Y)$
- Conditional entropy.
- Examples.

Suppose 'f' is a continuous function on the interval 'I'.

$$\sum_{i=1}^{n} a_i = 1 \quad \text{and} \quad a_i > 0;\ 1 \leq i \leq n$$

Then,

$$\sum_{i=1}^{n} a_i f(x_i) \leq f\left(\sum_{i=1} a_i x_i\right), \text{ where } x_i \in I,\ 1 \leq i \leq n.$$

Note :- Equality occurs iff $x_1 = x_2 = \cdots = x_n$.

(*) Theorem :-

Suppose 'x' is a R.V. having a probability distribution which takes on the values $p_1, p_2, \ldots p$ where $p_i > 0$, $1 \leq i \leq n$ — H/w proof

Then, $H(x) \leq \log_2 n$ [with equality iff $p_i = \frac{1}{n}$, $1 \leq i \leq n$

Pf :- $H(x) = -\sum_{i=1}^{n} p_i \log_2 p_i$

$$= \sum_{i=1}^{n} p_i \log_2 \frac{1}{p_i}$$

$$\leq \log_2 \left(\sum_{i=1}^{n} p_i \frac{1}{p_i} \right) = \log_2 n.$$

Theorem :-

H.W pf.

$H(x,y) \leq H(x) + H(y)$. and [equality holds iff x and y are independent.]

$$\boxed{\begin{array}{l} r_{ij} = P(X = x_i, Y = y_i). \\ H(x,y) = -\sum_{x}\sum_{y} r_{ij} \log_2 r_{ij} \end{array}} \longrightarrow (2)$$

Pf :- $X = x_i$, $1 \leq i \leq m$

$Y = y_j$, $1 \leq j \leq n$.

$p_i = P(X = x_i)$, $1 \leq i \leq m$.

$q_j = P(Y = y_j)$, $1 \leq j \leq n$.

$r_{ij} = P(X = x_i, Y = y_j)$.

Consider, $H(X,Y) - H(X) - H(Y)$.

Prove. $H(X,Y) - H(X) - H(Y) \leq 0$.

Marginal probability, $p_i = \sum_{j=1}^{n} r_{ij}$, $1 \leq i \leq m$.

$q_j = \sum_{i=1}^{n} r_{ij}$, $1 \leq j \leq n$.

$$H(x) + H(y) = -\left(\sum_{i=1}^{m} p_i \log_2 p_i + \sum_{j=1}^{n} q_j \log_2 q_j \right)$$

$$= -\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij} \log p_i + \sum_{j=1}^{n}\sum_{i=1}^{m} r_{ij} \log_2 q_j$$

$$= -\left(\sum_{i=1}^{m} \sum_{j=1}^{n} r_{ij} \log_2 p_i q_j \right) \longrightarrow ①$$

Apply Jensen's inequality for ① & ② eqn's.

(*) Note :-

$$H(x/y) = -\sum_{y} \sum_{x} P(y) \cdot P\left(\frac{x}{y}\right) \cdot \log_2 P(x/y)$$

$$\rightarrow \quad H(K/C) = -\sum_{y} \sum_{K} P(y) \cdot P(K/y) \cdot \log_2 P(K/y).$$

for a given 'C', how much that 'K' is uncertain.

$$\rightarrow \quad P(K/y) = \frac{P(K) \cdot P(y/K)}{P(y)}$$

$\Rightarrow$ Key equivocation

$\Downarrow$

uncertainity of 'K' given 'y'.

Eg :- $P = \{a, b, c\}$.

$K = \{K_1, K_2, K_3\}$.

$C = \{1, 2, 3, 4\}$.

Enc.

	a	b	c.
K1	1	2	3
K2	2	3	4
K3.	3.	4	1

$P(K_1) = P(K_2) = P(K_3) = 1/3$

$P(a) = 1/2$, $P(b) = 1/3$.

$P(c) = 1/6$

$$P(K_1/1) = \frac{P(K_1) \cdot P(1/K_1)}{P(1)}. \qquad \boxed{P(1) = \frac{2}{9}}$$

$$= \frac{1/3 \times P(1/K_1)}{2/9} = \frac{1/3 \times 1/2}{2/3} = 3/4$$

$$P(1/K_1) = P(x = D_{K_1}(y)).$$

$$= P(x = a) = 1/2$$

$$\cancel{P(K_1/2) = P(X = D_{K_1}(y))}$$

$$\cancel{= P(X = D_{K_1}(2))}.$$

$$\cancel{= P(X = b) = 1/3}$$

$$P(K_1/2) = \frac{P(K_1) \cdot P(2/K_2)}{P(2)} = ?$$

$P(K/y)$	1	2	3	4
K_1	3/4	2/5	1/6	0
K_2	0	3/5	1/3	1/3
K_3	1/4	0	1/2	2/3

$$H(K/y) = ?$$