Substitution

→ Substitution
→ Permutation.

Substitution cipher

Suppose S_n is a set of 'n' symbols.,

$\pi : S_n \to S_n$ is called permutation. if it is a bijective mapping.

$$\pi = (\pi(1), \pi(2), \ldots \pi(n)).$$

(or)

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix}.$$

Eg:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

i/p, o/p.

Note:-

S_n → set of all permutation with 'n' symbols of 'S'.

$S = \{1, 2, 3, \ldots n\}$.

Eg:-

$\Rightarrow f, g \in S_n$

$\Rightarrow$ $(f \circ g)(x) = f(g(x))$.

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$ → Ans

$(f \circ g)(1) = f(g(1))$.
$= f(1)$
$= 2$

$(f \circ g)(2) = f(g(2))$
$= f(3)$.
$= 3$

$(f \circ g)(3) = f(g(3))$
$= f(2)$.
$= 1$

$(f \circ g)(4) = f(g(4))$
$= f(4)$
$= 4$

Note :-

$fog \neq gof$. ⇒ composition is not commutative.

(*) Transposition cipher :-

$P = C = (Z_{26})^b$; b - size of message block.

(Key) K - set of all permutations over $(1, 2, \ldots, b)$.

$\pi = (\pi(1), \pi(2), \ldots \pi(b))$

π^{-1} ⇒ $\pi^{-1}(\pi(i)) = i, \forall i$

(inverse π)

⇒ block $(x_1, x_2, \ldots x_b) \in P$.

then encryption $e_\pi(x_1, x_2, \ldots x_b)$

$= (x_{\pi(1)}, x_{\pi(2)}, \ldots x_{\pi(b)})$.

decryption $d_\pi(y_1, y_2, \ldots y_b)$.

$= (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \ldots y_{\pi^{-1}(b)})$.

⇒ $y = f(x)$

$x = f^{-1}(y)$.

Eg :-

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

$$f^{-1} = \begin{pmatrix} 2 & 3 & 1 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$ → for 1 2 3 4 - i/p

written input in this order

$fof^{-1} = (1\ 2\ 3\ 4)$

1 2 3 4 → Key order.

Eg :- $K = (1\ 3\ 4\ 2)$.

$x =$ "a c d b"
$x_1\ x_2\ x_3\ x_4$

$y = ??$

Sol

$x = \begin{pmatrix} a & c & d & b \\ 1 & 3 & 4 & 2 \end{pmatrix}$

$y =$

$e_{m.k}(a\ c\ d\ b) = x_{K(1)} \cdot x_{K(2)} \cdot x_{K(3)} \cdot x_{K(4)}$.

$= x_1\ x_3\ x_4\ x_2$.

$= a\ d\ b\ c$.

$y_1\ y_2\ y_3\ y_4$

$x_{\pi(1)}$
$x_{\pi(2)}$
$x_{\pi(3)}$
$x_{\pi(4)}$.

$d_k(a\ d\ b\ c) = y_{K^{-1}(1)} \cdot y_{K^{-1}(2)} \cdot y_{K^{-1}(3)} \cdot y_{K^{-1}(4)}$

$= y_1\ y_4\ y_2\ y_3$

$= a\ c\ d\ b$. ✓

Eg :-

$\Rightarrow x = a\,c\,d\,b\ r\,s\,c\,d$.

Note :- → Transposition is not one-one substitution.

→ Here, 'c' will substitute with different letters.

(*) Binary operation :-

→ A '*' is called binary operation defined over non-empty 'S' if $a * b \in S$, $\forall a, b \in S$, we denote it with $(S, *)$.

Ex :- $(N, -) \Rightarrow$ non-binary operation over N.

Eg :- $3 - 4 \notin N$.

$(\mathbb{Z}, -) \Rightarrow$ yes, binary operation (not identity $3 - 0 = 0 - 3$)

Ex :- $(S_n, \circ) \Rightarrow$ yes, binary operation.

(composition of two permutation is always a permutation).

(*) Group :-

A non-empty set 'G' is binary operation with '*' is called a 'group' if it satisfy.

(i) Closure
(ii) Associative.
(iii) Identity.
(iv) Inverse.

Eg :- $(S_n, \circ) \Rightarrow$ group.

(*) Lagrange's theorem :-

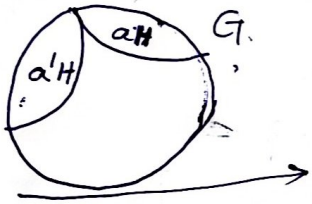
If 'G' is a group and 'H' is a subgroup of 'G', then $O(H) \mid O(G)$ (divides).

Pf :-

(i) for any $a \neq a'$, if $a \notin a'H$, then

$aH \cap a'H = \emptyset$.

(ii) $O(aH) = O(H)$.



we know that $a \notin a'H$

Consider,

$$a = ae = a(cc^{-1}).$$
$$= (ac).c^{-1} \longrightarrow (1)$$

Suppose $\exists\ b \in aH \cap a'H$.

So, $\exists\ c, c' \in H \ni ac = b = a'c'$

(1) Continue :

$$a = (ac).c^{-1}.$$
$$= b.c^{-1}.$$
$$= (a'c').c^{-1}.$$
$$= a'.(c'.c^{-1}).$$

$\therefore a \in a'H$. (Contradiction).

(ii) We have to prove $O(aH) = O(H)$.

Suppose $b, c \in aH$ with $b \neq c$., and.

$\Leftarrow ab = ac.$

Since, $\bar{a}^{-1}$ exists in G,

$$\bar{a}^{-1}(ab) = \bar{a}^{-1}(ac).$$
$$(\bar{a}^{-1}a).b = (\bar{a}^{-1}a).c.$$
$$\Rightarrow eb = ec. \Rightarrow \boxed{b = c} \Rightarrow \text{(Contradiction)}$$

$\therefore O(aH) = O(H)$.

$\Rightarrow O(H) \mid O(G)$

↓ divides.

Ex:- $(Z_4, +)$.

$Z_4 = \{0, 1, 2, 3\}$.

$H = \{0, 2\}$. ✓

$\Rightarrow Z_{12} = \{0, 1, 2, \ldots\ldots 11\}$.

$H_1 = \{0, 2, 4, 6, 8, 10\}$

$H_2 = \{0, 4, 8\}$.

(*) Quotient group :-

Let 'G' be a group (abelian). and $H \subseteq G$. The quotient group of 'G' modulo 'H' denoted by. 'G \ H', is the set of all cosets 'aH' with 'a' ranging over 'G', with the group operation. *, defined by. $(aH) * (bH) = abH$. and with the identity element being 'eH'.

(*) Cyclic groups :-

Let (G, H), be a group. we say that $a \in G$. is a generator of 'G' if

$G = \{a^n \mid n > 0, n \in \mathbb{Z}\}$. ⇒ denoted by. $G = \langle a \rangle$.

Ex :-

$Z_6 = \{0, 1, 2, 3, 4, 5\}$. , $(Z_6, +)$.

Nvidia apply cheyamanu ~~mail chidamanu~~.

$\Rightarrow$ $O(0) = 1$.
$O(1) = 6$.

$1^1 = 1$
$1^2 = 1+1 = 2$
$1^3 = 1+1+1 = 3$.
$1^4 = 4$
$1^5 = 5$
$1^6 = 6 \bmod 6 = 0$ $\Rightarrow$ cyclic.

$\{0,1,2,3,4,5\} \Rightarrow$ generator.

Ex:- $(Z_6^*, \times) \Rightarrow Z_6^* = \{1, 5\}$.

generator

$5^1 = 5$ ✓
$5^2 = 5 \times 5 = 25 \bmod 6$
$= 1$ ✓. $\Rightarrow$ cyclic.

Ex:- S_n = set of all permutations over n-symbols $\{1,2,3,\ldots,n\}$.

$S_3 = \{f_0, f_1, f_2, f_3, f_4, f_5\}$.

Not cyclic

(*) Any group is commutative then it is not a cyclic group.

(*) Discrete logarithm problem:- (DLP).

Let 'G' be a group. and $g \in G$. Finding smallest +ve integer 'K', for given 'h' $\in \langle g \rangle \Rightarrow h = g^K$

$$\boxed{K = \log_g(h).} \Rightarrow$$ (hard problem for large base values)

(*) $Z_n^* = \{ a \mid a \in Z_n \text{ and } \gcd(a, n) = 1 \}$. $\Rightarrow$ all invertible elements

$(Z_n^*, \times_n)$ is group / abelian grp.

Suppose, $n = pq$. where 'p' & 'q' are primes.

$\Downarrow$

(integer factorisation $\Rightarrow$ hard problem).

(*) Any element in Z_n^*, where $n = pq$. has an order dividing. LCM $(p-1, q-1)$.

(*) What is order of Z_n^* ?

$\Downarrow$

$O(Z_n^*) = \phi(n)$ $\longrightarrow$ Euler quotient.

$n = pq. \Rightarrow \phi(n) = (p-1)(q-1)$.

$\Downarrow$

$a \in Z_n^*$,

$a^{p-1} \bmod p = 1.$

$a^{q-1} \bmod q = 1.$

$\lambda = \text{lcm}(q-1, p-1).$

$p-1 \mid \lambda.$

$q-1 \mid \lambda.$

$a^{\lambda} \bmod p = 1$

$a^{\lambda} \bmod q = 1.$

(*) Ring:-

→ Let 'R' be a non-empty set and. binary operations are addition (+), multiplication (x). Then. $(R, +, x)$. is called, a 'Ring' if

① $(R, +)$. is abelion grp.

② (R, x) is closure, & associative.

③ Distributive laws.: $a \times (b+c) = a \times b + a \times c$.

$(a+b) \times c = a \times c + b \times c$.

* Eg:- $S = \{0, \pm 2, \pm 4, \ldots\}$.

$(S, +, \times)$.

① $(S, +)$ → it is a abelion grp.
② $(S, \times)$ → closure & associative.
③ Distributive laws:

→ Ring with Commutative (no identity)

commutative ?? (yes).

identity exists w.r.t "x" exists ?? (No) ↓ ('S' doesnot contains '1')

Eg:-

Set of n-square matrices.

(i) Matrix addition. ⇒ abelion.

(ii) Matrix multiplication ⇒ closure, associative.

↓↓

Ring with identity. (no commutative)

* Integral domain:-

~~A ring with the following commutative.~~

A commutative ring. $(R, +, \times)$, with the following properties:

(i) Multiplicative identity:

(ii) No zero divisors: if $a, b \in R$ and $ab = 0$.

then $a = 0$, (or) $b = 0$.

Eg:- $Z_6 = \{0, 1, 2, 3, 4, 5\}$, $+_6$, $\times_6$.

$a = 3$, $b = 4$.

$ab = 3 \times 4 = 12 \bmod 6 = 0$; ⇒ 3, 4 zero divisors.

Note:-

→ whenever an element is a zero divisor then inverse does not exists.

Eg:-

→ contd...

Here, '3' and '4' are not co-primes to '6'. (non-invertible elements).

- $Z_5 = \{0, 1, 2, 3, 4\}$: $+_5$, $+_6$

  ⇓

  here, all non-zero elements co-prime to '5'. So, inverse exists.

Eg:-

$(Z, +, \times)$ → integral domain. ??

⊛ Field:-

We say $(F, +, \times)$ is a field. if it is an integral domain with all non-zero elements are invertible.

Ex:- $(\mathbb{R}, +, \times)$ → field.

$(Z_p, +_p, \times_p)$ where 'p' is prime → field.

'p' is not prime → ring.

$(C, +, \times)$

↓

Complex

Generator:-

$(G, *)$ - group.

$g \in G$, $G = \langle g \rangle$.

⊛ Polynomial over $\mathbb{R}$:-

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad ; \quad a_i \in \mathbb{R}$$

$$g(x) = \sum_{i=0}^{m} b_i x^i \quad ; \quad b_i \in \mathbb{R}.$$

Eg :- $f(x) = x^2 + 1$.

$g(x) = x^3 + x + 2$.

$f(x) + g(x) = x^3 + x^2 + x + 3$.

$f(x) \cdot g(x) = ??$

⊛ Irreducible polynomial :-

$f(x)$ over a field 'F' is called irreducible, if there exists no root in 'F' (or) we cannot write it as a product of lower degree polynomials.

'α' is a root of $f(x)$.

$(x - \alpha)$ is a factor.

$f(x) = (x - \alpha) \cdot g(x)$.

Eg :- $f(x) = x^2 + 1$ over $\mathbb{Z}_2 = \{0, 1\}$.

$f(1) = 1^2 + 1 = 2 \bmod 2$

$= 0$.

$f(x) = (x+1) \cdot (x+1)$.

⊛ G.F :- (Galois field).

Set of all polynomials of degree $(n-1)$. (or) less over the field $\mathbb{Z}_p$ forms a field. modulo an irreducible polynomial $m(x)$ of degree 'n'.

Note:-

Order of G.F(p^n) is p^n.

(i) G.F(p) is called prime field.

(ii) GF(2^n) is called binary field.

Eg:- G.F(2^3).

$O(G.F(2^3)) = 2^3 = 8$.

$Z_2 = \{0, 1\}$.

$f(x) = a_2x^2 + a_1x + a_0$.

$a_2 a_1 a_0$.

0 - 000
1 - 001
2 - 010
⋮
6 - 110
7 - 111

Eg:- $f = 2$ $\quad f+g = ??$

$g = 5$

$$\begin{array}{r} 010 \\ 101 \\ \hline 111 \end{array} \Rightarrow 7.$$

$f = 4$

$g = 6$.

$$\begin{array}{r} 100 \\ 110 \\ \hline 001 \end{array} \Rightarrow 2$$

$f.g = ??$

$4 \times 6 = 24 \bmod 8$

$= 0$.

Eg:- $f = 2 \Rightarrow 010$

$g = 5 \Rightarrow 101$

$f = x$

$g = x^2 + 1$

$f \cdot g = x^3 + x \mod m(x) = ??$

$\Rightarrow 110 = 6$

Eg:- $f = 4 = 100 = x^2$

$g = 6 = 110 = x^2 + x$

GF(2^3) over $m(x) = x^3 + x + 1$.

$f \cdot g = x^4 + x^3 \mod m(x)$.

$= (x^4 + x^3) \mod (x^3 + x + 1)$

$$x^3 + x + 1 \;\big)\; x^4 + x^3 \;\big(\; x + 1$$

$x^4 + x^2 + x$

$x^3 + x^2 + x$

$x^3 + x + 1$

$x^2 + 1$

$\Rightarrow f \cdot g = x^2 + 1$

$= 5$

(*) gcd $(f(x), g(x)) = ??$, then find inverse $(f(x)) = ??$

Eg:- AES used:

GF(2^8). over $m(x) = x^8 + x^4 + x^3 + x + 1$.

(*) Let F_{p^n} is a field, (there exists G.F.)

→ $(F_{p^n})^*$ is a cyclic group, over multiplication.

→ A generator of $(F_{p^n})^*$ is called primitive root.