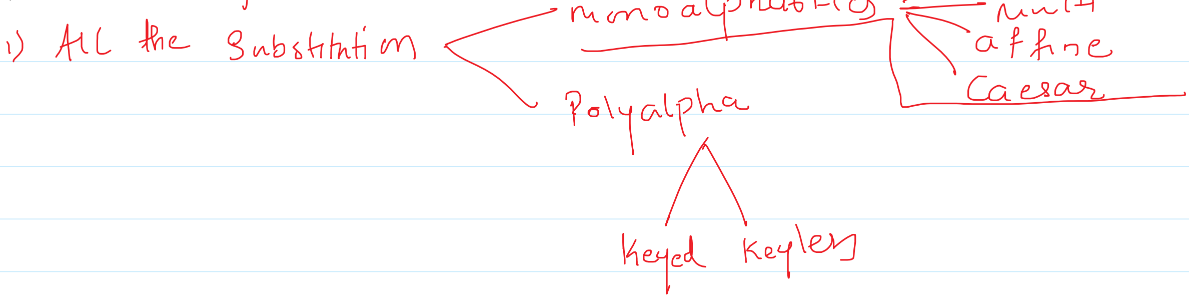
Substitution cipher

23 July 2021 13:15



Exp 2 :- To implement multiplicative Cipher (affine) using java

ex :- Plain text = name (str) __
$\quad\quad\quad$ P

Key = 7 __

multiplicative

```
enter the plain text:
name
enter the Key
7
encrypted text is : "___"
decrypted text is : "___"
```

algorithm :-

1) $C = (P \times K) \bmod 26$

P =	n	a	m	e
	13	0	12	4

$C_1 = (13 \times 7) \bmod 26$
$= 91 \bmod 26 = 13$

$C_2 = (0 \times 7) \bmod 26$
$= 0 \bmod 26 = 0$

$C_3 = (12 \times 7) \bmod 26$
$= 84 \bmod 26 = 6$

$C_4 = (4 \times 7) \bmod 26$
$= 28 \bmod 26 = 2$

C =	13	0	6	2
CT =	n	a	g	c

PT = name
CT = $\boxed{\text{nagc}}$

Decryption :-

CT = nagc
K^{-1} = ?
PT = ?

1) CT =	n	a	g	c
	13	0	6	2

2) $K^{-1} = 15$

$k = 7 = (a)$

$= (\cancel{e} \times \underline{a}^{-1}) \bmod 26$

$7 = K^{-1}$

x od 26 = 1 mod 26

o x x mod 26 = 1 mod 26

$7x \bmod 26 = 1$

- extended euclidean alg = $\underline{\text{fwd}} + \underline{\text{rev}}$

multiplicative inverse

1) Divident = divisor (q) + r

forward

$26 = 7 \times 3 + 5$ — (a)

$7 = 5(1) + \boxed{2}$ — (b)

$5 \,\big)\, 7$
$\underline{5}$
2

$5 = 2 \times 2 + 1$ — $\cancel{(b)}$ (c)

$\boxed{2 = 1 \times 2 + \textcircled{0}}$ — $\cancel{(d)}$

Skip

reverse

Rewrite eq^n (c)

$5 = 2(2) + (1)$

$1 = 5 - \textcircled{2}\textcircled{2}$

$= 5 + \textcircled{2}(-2)$ — ①

Snbs ⓑ in ①

$1 = 5 + [7 + 5(-1)](-2)$

$= \underline{5(1)} + [7 + 5(-1)](-2)$

$= 7(-2) + 5\underline{(1)} + 5\underline{(2)}$

$= 7(-2) + 5(3)$ — ②

Sub ⓐ in ②

$1 = 7(-2) + [26 + 7(-3)](3)$

$= 7(-2) + 26(3) + 7(-9)$

$1 = \textcircled{7}(\textcircled{-11}) + \cancel{26(3)}$

$7 \times (-)$ $K^{-1} = +\underline{11}$ $= 26 + (-11) =$
$26 - 11 = 15$

$\underline{\underline{-11}}$ ✓ $= 26 + (-11) = 26 - 11 = \underline{\underline{15}}$

$\underline{\underline{k = 19}}$

Forward = ⑲/26

$26 = 19(1) + 7$ — ①

Reverse

$1 = 5 + 2(-2)$ — (a)

$26 = 19(1) + 1$ — ①

$19 = 7(2) + \underline{5}$ — ②

$7 = 5(1) + 2$ — ③

$5 = 2(2) + 1$ — ④

$\boxed{2 = 1(2) + 0 \quad — ⑤}$ x

$1 = 5 + 2(-2)$ — (a)

eq^n ③ in ⓐ

$1 = \overset{\uparrow}{5} + [7 + 5(-1)](-2)$

$= (5 \times 1) + [7 + 5(-1)](-2)$

$= 5(\times 1) + 7(-2) + 5(2)$

$= 5(3) + 7(-2)$ — (b)

eq^n ② in ⓑ

$1 = 5(3) + 7(-2)$

$= [19 + 7(-2)](3) + 7(-2)$

$= 19(3) + 7(-6) + 7(-2)$

$1 = 19(3) + 7(-8)$ — (c)

eq^n ① in (c)

$1 = 19(3) + [26 + 19(-1)](-8)$

$= \underline{19(3)} + \underline{26(-8)} + \underline{19(8)}$

$1 = \underline{9}(\boxed{11}) + \cancel{26(-8)}$

$\downarrow$

$K \times \underline{11} = 1 \bmod 26$

$K = 19,\ K^{-1} = 11$

CT = n a g c

13 0 6 2

$K^{-1} = 15$

$P_1 = (CT \times K^{-1}) \bmod 26$

$= (13 \times 15) \bmod 26$

$= 195 \bmod 26$

$= 13$

$P_2 = (C_2 \times K^{-1}) \bmod 26$

$= (0 \times 15) \bmod 26$

$= 0 \bmod 26$

$= 0$

$P_3 = (C_3 \times K^{-1}) \bmod 26$

$= (6 \times 15) \bmod 26$

$= 90 \bmod 26$

$= 12$

$P_4 = ((C_4 \times K^{-1}) \bmod 26$

$= (2 \times 15) \bmod 26$

$= 30 \bmod 26$

$= 4$

PT = 13 0 12 4

↓ ↓ ↓ ↓

n a m e

PT = name

affine cipher → Hybrid of additive & multiplicative

rules	rules
$E = (P + K) \bmod 26$	$E = (P \times K) \bmod 26$
$D = (P - K) \bmod 26$	$D = (P \times K^{-1}) \bmod 26$

K_2 = additive

K_1 = multiplicative

P

$$E = (\underbrace{(P \times K_1)}_{P_1} + \underbrace{K_2}_{+ K_2}) \bmod 26$$

1) multiply PT with multiplicative key (answer)
2) Now add answer with additive key (ans1)
3) Perform modulo function of ans 1 with 26 (36)

Decryption :-

$$D = [(P \times K_1^{-1}) - K_2) \bmod 26$$

K^{-1} = multiplicative inverse of K_1

$-K_2$ = additive inverse of K_2

$$\left[\begin{array}{l} K_2 = \\ 3 = -3 \\ -11 = +11 \end{array}\right]$$

$$K(\overset{\overset{\text{mult}}{a}}{7}, \overset{\overset{\text{additive}}{b}}{3})$$

K = 7

2) q r_1 r_2 r t_1 t_2 t

$7 \times \boxed{\cdot} \bmod 26 = \boxed{1}$

0|1|2|3 ○ - /25

0 → 25