Fadhillah Akbar I

140810190068

Praktikum Kriptografi

Exercise

FORTRAN key 20

5 14 17 19 17 0 13 -> X+20 mod 26

= 25| 34mod26 |31mod26 |33mod26 |31mod26 |40mod26 |27mod26

= 25 8 11 13 11 20 7 => ZILNLUH

ZGXEIDZJN key 15

25 6 23 4 8 3 25 9 13 -> X-15 mod 26

= 10 |-9mod26| 8 |-11mod26 |-7mod26 |-12mod26 |10| -6mod26| -2mod26

= 10 17 8 15 19 14 10 20 24 => KRIPTOKUY

TNZCNATXNA key 13 (ROT13)

19 13 25 2 13 0 19 23 13 0 -> X-13 mod 26

= 6 |0 |12| -11mod26| 0 |-13mod26 |6 |10|0|-13mod26

= 6 0 12 15 0 13 6 10 0 13 => GAMPANGKAN

Tugas nomor 2

Tentukan kalimat min 3 kata 15 huruf dan enkripsikan dengan affine cipher lalu deskripsikan kembali

Kalimat : apex legend is trash

KEY : (19,0)

A -> E(0) = (19(0)+0) mod 26 = 0 mod 26 = 0 -> A

P -> E(15) = (19(15)+0) mod 26 = 285 mod 26 = 25 -> Z

E -> E(4) = (19(4)+0) mod 26 = 76 mod 26 = 24 -> Y

X -> E(23) = (19(23)+0) mod 26 = 437 mod 26 = 21 -> V

L -> E(11) = (19(11)+0) mod 26 = 209 mod 26 = 1 - > B

E -> E(4) = (19(4)+0) mod 26 = 76 mod 26 = 24 -> Y

G -> E(6) = (19(6)+0) mod 26 = 114 mod 26 = 10 -> K

E -> E(4) = (19(4)+0) mod 26 = 76 mod 26 = 24 -> Y

N -> E(13) = (19(13)+0) mod 26 = 247 mod 26 = 13 -> N

D -> E(3) = (19(3)+0) mod 26 = 57 mod 26 = 5 ->F

I -> E(8) = (19(8)+0) mod 26 = 152 mod 26 = 22 -> W

S -> E(18) = (19(18)+0) mod 26 = 342 mod 26 = 4 -> E

T -> E(19) = (19(19)+0) mod 26 = 361 mod 26 = 23 -> X

R -> E(17) = (19(17)+0) mod 26 = 323 mod 26 = 11 -> L

A -> E(0) = (19(0)+0) mod 26 = 0 mod 26 = 0 -> A

S -> E(18) = (19(18)+0) mod 26 = 342 mod 26 = 4 -> E

H -> E(7) = (19(7)+0) mod 26 = 133 mod 26 = 3 - > D

APEX LEGEND IS TRASH -> affineCipherEncrypt(19,0) -> AZYV BYKYNF WE XLAED

Gcd(19,26) =

26 = 19 x 1 + 7

19 = 7 x 2 + 5

7 = 5 x 1 + 2

5 = 2 x 2 + 1

2 = 1x2 + 0

$t_0 = 0$,$t_1 = 1$

$t_2 = 0 – (1 \times 1) \bmod 26 = -1 \bmod 26 = 25$

$t_3 = 1-(25 \times 2) \bmod 26 = -49 \bmod 26 = 3$

$t_4 = 25 – (3x1) \bmod 26 = 22 \bmod 26 = 22$

$t_5 = 3 – (22 \times 2) \bmod 26 = -41 \bmod 26 = 11$

$a^{-1} = 11$

A -> D(0) = 11 (0-0) mod 26 = 0 mod 26 = 0 -> A

Z - > D(25) = 11(25-0) mod 26 = 275 mod 26 = 15 -> P

Y-> D(24) = 11(24-0) mod 26 = 264 mod 26 = 4 - > E

V -> D(21) = 11(21-0) mod 26 = 231 mod 26 = 23 - > X

B -> D(1) = 11 (1-0) mod 26 = 11 mod 26 = 11 -> L

Y-> D(24) = 11(24-0) mod 26 = 264 mod 26 = 4 - > E

K-> D(10) = 11 (10-0) mod 26 = 11 mod 26 = 6 -> G

Y-> D(24) = 11(24-0) mod 26 = 264 mod 26 = 4 - > E

N -> D(13) = 11 (13-0) mod 26 = 143 mod 26 = 13 -> N

F-> D(5) = 11 (5-0) mod 26 = 55 mod 26 = 3 -> D

W -> D(22) = 11 (22-0) mod 26 = 242 mod 26 = 8 -> I

E -> D(4) = 11 (4-0) mod 26 = 44 mod 26 = 18 -> S

X -> D(23) = 11 (23-0) mod 26 = 253 mod 26 = 19 -> T

L -> D(11) = 11 (11-0) mod 26 = 121 mod 26 = 17 - > R

A -> D(0) = 11 (0-0) mod 26 = 0 mod 26 = 0 -> A

E -> D(4) = 11 (4-0) mod 26 = 44 mod 26 = 18 -> S

D -> D(3) = 11 (3-0) mod 26 = 33 mod 26 = 7 - > H

AZYV BYKYNF WE XLAED -> affineCipherDecrypt(19,0) -> APEX LEGEND IS TRASH