Nama : Vernandika Stanley Hansen
NPM : 140810220031
Praktikum Kriptografi

Tugas 2

Enkripsikan nama lengkap anda menggunakan Affine Cipher dan kembalikan menjadi plainteks, **a=9 b=[2 digit NPM akhir]**.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

a = 9
b = 31
E(x) = (ax + b) mod 26
D(y) = a^{-1} (y - b) mod 26

ENKRIPSI

VERNANDIKA = 21 4 17 13 0 13 3 8 10 0

STANLEY = 18 19 0 13 11 4 24

HANSEN = 7 0 13 18 4 13

E(21) = (9 * 21 + 31) mod 26 = 220 mod 26 = 12 ⇒ M

E(4) = (9 * 4 + 31) mod 26 = 67 mod 26 = 15 ⇒ P

E(17) = (9 * 17 + 31) mod 26 = 184 mod 26 = 2 ⇒ C

E(13) = (9 * 13 + 31) mod 26 = 148 mod 26 = 18 ⇒ S

E(0) = (9 * 0 + 31) mod 26 = 31 mod 26 = 5 ⇒ F

E(13) = (9 * 13 + 31) mod 26 = 148 mod 26 = 18 ⇒ S

E(3) = (9 * 3 + 31) mod 26 = 58 mod 26 = 6 ⇒ G

E(8) = (9 * 8 + 31) mod 26 = 103 mod 26 = 25 ⇒ Z

E(10) = (9 * 10 + 31) mod 26 = 121 mod 26 = 17 ⇒ R

E(0) = (9 * 0 + 31) mod 26 = 31 mod 26 = 5 ⇒ F

VERNANDIKA ⇒ MPCSFSGZRF

E(18) = (9 * 18 + 31) mod 26 = 193 mod 26 = 11 ⇒ L

E(19) = (9 * 19 + 31) mod 26 = 220 mod 26 = 20 ⇒ U

E(0) = (9 * 0 + 31) mod 26 = 31 mod 26 = 5 ⇒ F

E(13) = (9 * 13 + 31) mod 26 = 148 mod 26 = 18 ⇒ S

E(11) = (9 * 11 + 31) mod 26 = 130 mod 26 = 0 ⇒ A

E(4) = (9 * 4 + 31) mod 26 = 67 mod 26 = 15 ⇒ P

E(24) = (9 * 24 + 31) mod 26 = 247 mod 26 = 13 ⇒ N

STANLEY ⇒ LUFSAPN

E(7) = (9 * 7 + 31) mod 26 = 94 mod 26 = 16 ⇒ Q

E(0) = (9 * 0 + 31) mod 26 = 31 mod 26 = 5 ⇒ F

E(13) = (9 * 13 + 31) mod 26 = 148 mod 26 = 18 ⇒ S

E(18) = (9 * 18 + 31) mod 26 = 193 mod 26 = 11 ⇒ L

E(4) = (9 * 4 + 31) mod 26 = 67 mod 26 = 15 ⇒ P

E(13) = (9 * 13 + 31) mod 26 = 148 mod 26 = 18 ⇒ S

HANSEN ⇒ QFSLPS

VERNANDIKA STANLEY HANSEN ⇒ MPCSFSGZRF LUFSAPN QFSLPS

DEKRIPSI

Mencari a^{-1} =

GCD(a, m)

GCD(9, 26)

26 = 9 * 2 + 8

9 = 8 * 1 + 1

$8 = 1 * 8 + 0$

$t0 = 0, t1 = 1$

$t2 = (to - (q1 * t1)) \bmod 26 = (0 - (2 * 1)) \bmod 26 = -2 \bmod 26 = 24$

$t3 = (t1 - (q2 * t2)) \bmod 26 = (1 - (1 * 24)) \bmod 26 = -23 \bmod 26 = 3$

$a^{-1} = 3$

MPCSFSGZRF = 12 15 2 18 5 18 6 25 17 5

LUFSAPN = 11 20 5 18 0 15 13

QFSLPS = 16 5 18 11 15 18

$D(12) = 3(12 - 31 + 26) \bmod 26 = 21 \bmod 26 = 21 \Rightarrow V$

$D(15) = 3(15 - 31 + 26) \bmod 26 = 30 \bmod 26 = 4 \Rightarrow E$

$D(2) = 3(2 - 31 + 26 + 26) \bmod 26 = 69 \bmod 26 = 17 \Rightarrow R$

$D(18) = 3(18 - 31 + 26) \bmod 26 = 39 \bmod 13 = 4 \Rightarrow N$

$D(5) = 3(5 - 31 + 26) \bmod 26 = 0 \bmod 26 = 0 \Rightarrow A$

$D(18) = 3(18 - 31 + 26) \bmod 26 = 39 \bmod 13 = 4 \Rightarrow N$

$D(6) = 3(6 - 31 + 26) \bmod 26 = 3 \bmod 13 = 3 \Rightarrow D$

$D(25) = 3(25 - 31 + 26) \bmod 26 = 60 \bmod 13 = 8 \Rightarrow I$

$D(17) = 3(17 - 31 + 26) \bmod 26 = 36 \bmod 10 = 4 \Rightarrow K$

$D(5) = 3(5 - 31 + 26) \bmod 26 = 0 \bmod 26 = 0 \Rightarrow A$

MPCSFSGZRF $\Rightarrow$ VERNANDIKA

$D(11) = 3(11 - 31 + 26) \bmod 26 = 18 \bmod 26 = 18 \Rightarrow S$

$D(20) = 3(20 - 31 + 26) \bmod 26 = 45 \bmod 26 = 19 \Rightarrow T$

$D(5) = 3(5 - 31 + 26) \bmod 26 = 0 \bmod 26 = 0 \Rightarrow A$

$D(18) = 3(18 - 31 + 26) \bmod 26 = 39 \bmod 26 = 13 \Rightarrow N$

$D(0) = 3(0 - 31 + 26 + 26) \bmod 26 = 63 \bmod 26 = 11 \Rightarrow L$

$D(15) = 3(15 - 31 + 26) \bmod 26 = 30 \bmod 26 = 4 \Rightarrow E$

$D(13) = 3(13 - 31 + 26) \bmod 26 = 24 \bmod 26 = 24 \Rightarrow Y$

LUFSAPN ⇒ STANLEY

D(16) = 3(16 - 31 + 26) mod 26 = 33 mod 26 = 7 ⇒ H

D(5) = 3(5 - 31 + 26) mod 26 = 0 mod 26 = 0 ⇒ A

D(18) = 3(18 - 31 + 26) mod 26 = 39 mod 26 = 13 ⇒ N

D(11) = 3(11 - 31 + 26) mod 26 = 18 mod 26 = 18 ⇒ S

D(15) = 3(15 - 31 + 26) mod 26 = 30 mod 26 = 4 ⇒ E

D(18) = 3(18 - 31 + 26) mod 26 = 39 mod 26 = 13 ⇒ N

QFSLPS ⇒ HANSEN

MPCSFSGZRF LUFSAPN QFSLPS ⇒ VERNANDIKA STANLEY HANSEN