Nama : Ibrahim Dafi Iskandar

NPM : 140810210039

Kelas : A

**Tugas 2 Praktikum Kriptografi**

**Enkripsikan nama lengkap anda menggunakan Affine Cipher dan kembalikan menjadi plainteks,**

**a=9 b=[2 digit NPM akhir]**

**Jawab:**

Nama = IBRAHIM DAFI ISKANDAR

a = 9

b = 39

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| I | B | R | A | H | I | M | D | A | F | I | I | S | K | A | N | D | A | R |
| 8 | 1 | 17 | 0 | 7 | 8 | 12 | 3 | 0 | 5 | 8 | 18 | 10 | 0 | 0 | 13 | 3 | 0 | 17 |

**Enkripsi**

E(8) = (9(8) + 39) mod 26 = 7 => H

E(1) = (9(1) + 39) mod 26 = 22 => W

E(17) = (9(17) + 39) mod 26 = 10 => K

E(0) = (9(0) + 39) mod 26 = 13 => N

E(7) = (9(7) + 39) mod 26 = 24 => Y

E(8) = (9(8) + 39) mod 26 = 7 => H

E(12) =(9(8) + 39) mod 26 =12 🡪R

E(3) = (9(3) + 39) mod 26 = 14 => O

E(0) = (9(0) + 39) mod 26 = 13 => N

E(5) = (9(5) + 39) mod 26 = 6 => G

E(8) = (9(8) + 39) mod 26 = 7 => H

E(8) = (9(8) + 39) mod 26 = 7 => W

E(10) = (9(10) + 39) mod 26 = 19 => D

E(0) = (9(0) + 39) mod 26 = 25 => Y

E(0) = (9(0) + 39) mod 26 = 13 => E

E(13) = (9(13) + 39) mod 26 = 0 => X

E(3) =(9(3)+39)mod 26 =14 🡪O

E(0) =(9(0)+39)mod 26 =13 🡪N

E(17) =(9(17)+39)mod 26 =10 🡪K

Hasil enkripsi (E) = HWKNYHR ONGH WDYEXONK

**Dekripsi**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| H | W | K | N | Y | H | R | O | N | G | H | H | T | Z | N | A | O | N | K |
| 7 | 22 | 10 | 13 | 24 | 7 | 17 | 14 | 13 | 6 | 7 | 7 | 19 | 25 | 13 | 0 | 14 | 13 | 10 |

gcd(9,26)

26 = 9 \* 2 + 8

9 = 8 \* 1 + 1

8 = 1 \* 8 + 0

t0 = 0

t1 = 1

t2 = (0 - (2\*1)) mod 26 = -2 mod 26 = 24

t3 = (1 - (1\*24)) mod 26 = -23 mod 26 = 3

a-1 = 3

D(7) = 3(7 - 39) mod 26 = 8 => I

D(1) = 3(1 - 39) mod 26 = 1 => B

D(17) = 3(10 - 39) mod 26 = 17 => R

D(13) = 3(13 - 39) mod 26 = 8 => A

D(24) = 3(24 - 39) mod 26 = 7 => H

D(7) = 3(7 - 39) mod 26 = 8 => I

D(17) =(3(17-39)mod 26 =12 🡪12

D(14) = 3(14 - 39) mod 26 = 3 => D

D(13) = 3(13 - 39) mod 26 = 0 => A

D(6) = 3(6 - 39) mod 26 = 5 => F

D(7) = 3(7 - 39) mod 26 = 8 => I

D(7) = 3(7 - 39) mod 26 = 8 => I

D(19) = 3(19 - 39) mod 26 = 18 => S

D(25) = 3(25 - 39) mod 26 = 10 => K

D(13) = 3(13 - 39) mod 26 = 0 => A

D(0) = 3(0 - 39) mod 26 = 13 => N

D(14) = 3(14 - 39) mod 26 = 3 🡪D

D(13) = 3(13 - 39) mod 26 = 0 🡪A

D(10) = 3(10 - 39) mod 26 = 17 🡪R

Hasil dekripsi (D) = IBRAHIM DAFI ISKANDAR