Nama : Salsabila Karin

NPM : 140810190015

Praktikum Kriptografi A

TUGAS-1

Exercise

Shift cipher

1. FORTRAN

   key 20

   5 14 17 19 17 0 13 => (k + 20) mod 26

   F = 25

   O = 34mod26

   R = 31mod26

   T = 33mod26

   R = 31mod26

   A = 40mod26

   N = 27mod26

   = 25 8 11 13 11 20 7 => ZILNLUH

   ZGXEIDZJN

   key 15

   25 6 23 4 8 3 25 9 13 => (k – 20) mod 26

   Z = 10

   G = -9mod26

   X = 8

   E = -11mod26

   I = -7mod26

   D = -12mod26

   Z = 10

J = -6mod26

N = -2mod26

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

2. TNZCNATXNA
   ROT 13

   19 13 25 2 13 0 19 23 13 0

   Dikurang 13 (-13)

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

Tugas

Key : (15, 2)

Enkripsi

Plaintext: AKU SENANG KULIAH

A => E(0) = (15(0) + 2) mod 26 = 2 mod 26 = 2 => C

K => E(10) = (15(10) + 2) mod 26 = 152 mod 26 = 22 => W

U => E(20) = (15(20) + 2) mod 26 = 302 mod 26 = 16 => Q

S => E(18) = (15(18) + 2) mod 26 = 272 mod 26 = 12 => M

E => E(4) = (15(4) + 2) mod 26 = 62 mod 26 = 10 => K

N => E(13) = (15(13) + 2) mod 26 = 197 mod 26 = 15 => P

A => E(0) = (15(0) + 2) mod 26 = 2 mod 26 = 2 => C

N => E(13) = (15(13) + 2) mod 26 = 197 mod 26 = 15 => P

G => E(6) = (15(6) + 2) mod 26 = 92 mod 26 = 14 => O

K => E(10) = (15(10) + 2) mod 26 = 152 mod 26 = 22 => W

U => E(20) = (15(20) + 2) mod 26 = 302 mod 26 = 16 => Q

L => E(11) = (15(11) + 2) mod 26 = 167 mod 26 = 11 => L

I => E(8) = (15(8) + 2) mod 26 = 122 mod 26 = 18 => S

A => E(0) = (15(0) + 2) mod 26 = 2 mod 26 = 2 => C

H => E(7) = (15(7) + 2) mod 26 = 107 mod 26 = 3 => D

AKU SENANG KULIAH => E(x) => CWQ MKPCPO WQLSCD

Deskripsi

Gcd(15,26) =

26 = 15 x 1+ 11

15 = 11 x 1 + 4

11 = 4 x 2 + 3

4 = 3 x 1 + 1

3 = 1 x 3 + 0

$t_0 = 0$ $t_1 = 1$

t_2 = (0 – (1 . 1)) mod 26 = -1 mod 26 = 25

t_3 = (1 – (1 . 25)) mod 26 = -24 mod 26 = 2

t_4 = (25 – (2 . 2)) mod 26 = 21 mod 26 = 21

t_5 = (2 – (1 . 21)) mod 26 = -19 mod 26 = 7

C => D(2) = 7(2 – 2) mod 26 = 0 mod 26 = 0 => A

W => D(22) = 7(22 – 2) mod 26 = 140 mod 26 = 10 => K

Q => D(16) = 7(16 – 2) mod 26 = 98 mod 26 = 20 => U

M => D(12) = 7(12 – 2) mod 26 = 70 mod 26 = 18 => S

K => D(10) = 7(10 – 2) mod 26 = 56 mod 26 = 4 => E

P => D(15) = 7(15 – 2) mod 26 = 91 mod 26 = 13 => N

C => D(2) = 7(2 – 2) mod 26 = 0 mod 26 = 0 => A

P => D(15) = 7(15 – 2) mod 26 = 91 mod 26 = 13 => N

O => D(14) = 7(14 – 2) mod 26 = 84 mod 26 = 6 => G

W => D(22) = 7(22 – 2) mod 26 = 140 mod 26 = 10 => K

Q => D(16) = 7(16 – 2) mod 26 = 98 mod 26 = 20 => U

L => D(11) = 7(11 – 2) mod 26 = 63 mod 26 = 11 => L

S => D(18) = 7(18 – 2) mod 26 = 112 mod 26 = 8 => I

C => D(2) = 7(2 – 2) mod 26 = 0 mod 26 = 0 => A

D => D(3) = 7(3 – 2) mod 26 = 7 mod 26 = 7 => H

CWQ MKPCPO WQLSCD => D(y) => AKU SENANG KULIAH