

Nama : Kefilino Khalifa Filardi

NPM : 140810180028

Kelas : B

Tugas Praktikum Kriptografi Pertemuan #2

1. Soal No-1 : Exercises

Plaintext = ECLIPSE, K = 18

$E = 4, E(4) = (4 + 18) \bmod 26 = 22 \bmod 26 = 22 = W$
 $C = 2, E(2) = (2 + 18) \bmod 26 = 20 \bmod 26 = 20 = U$
 $L = 11, E(11) = (11 + 18) \bmod 26 = 29 \bmod 26 = 3 = D$
 $I = 8, E(8) = (8 + 18) \bmod 26 = 26 \bmod 26 = 0 = A$
 $P = , E(15) = (15 + 18) \bmod 26 = 33 \bmod 26 = 7 = H$
 $S = , E(18) = (18 + 18) \bmod 26 = 36 \bmod 26 = 10 = K$
 $E = , E(4) = (4 + 18) \bmod 26 = 22 \bmod 26 = 22 = W$

Ciphertext = WUDAHKW

Plaintext = WYHRRYPWAVRLYLUQVD, K = 7

$W = 22, E(22) = (22 - 7) \bmod 26 = 15 \bmod 26 = 15 = P$
 $Y = 24, E(24) = (24 - 7) \bmod 26 = 17 \bmod 26 = 17 = R$
 $H = 7, E(7) = (7 - 7) \bmod 26 = 0 \bmod 26 = 0 = A$
 $R = 17, E(17) = (17 - 7) \bmod 26 = 10 \bmod 26 = 10 = K$
 $R = 17, E(17) = (17 - 7) \bmod 26 = 10 \bmod 26 = 10 = K$
 $Y = 24, E(24) = (24 - 7) \bmod 26 = 17 \bmod 26 = 17 = R$
 $P = 15, E(15) = (15 - 7) \bmod 26 = 8 \bmod 26 = 8 = I$
 $W = 22, E(22) = (22 - 7) \bmod 26 = 15 \bmod 26 = 15 = P$
 $A = 0, E(0) = (0 - 7) \bmod 26 = -7 \bmod 26 = 19 = T$
 $V = 21, E(21) = (21 - 7) \bmod 26 = 14 \bmod 26 = 14 = O$
 $R = 17, E(17) = (17 - 7) \bmod 26 = 10 \bmod 26 = 10 = K$
 $L = 11, E(11) = (11 - 7) \bmod 26 = 4 \bmod 26 = 4 = E$
 $Y = 24, E(24) = (24 - 7) \bmod 26 = 17 \bmod 26 = 17 = R$
 $L = 11, E(11) = (11 - 7) \bmod 26 = 4 \bmod 26 = 4 = E$
 $U = 20, E(20) = (20 - 7) \bmod 26 = 13 \bmod 26 = 13 = N$
 $Q = 16, E(16) = (16 - 7) \bmod 26 = 9 \bmod 26 = 9 = J$
 $V = 21, E(21) = (21 - 7) \bmod 26 = 14 \bmod 26 = 14 = O$
 $D = 3, E(3) = (3 - 7) \bmod 26 = -4 \bmod 26 = 22 = W$

Ciphertext = PRAKKRIPTOKERENJOW

Plaintext = VSRFGUNPRC, ROT13

V = 21, $E(21) = (21 - 13) \bmod 26 = 8 \bmod 26 = 8 = I$
S = 18, $E(18) = (18 - 13) \bmod 26 = 5 \bmod 26 = 5 = F$
R = 17, $E(17) = (17 - 13) \bmod 26 = 4 \bmod 26 = 4 = E$
F = 5, $E(5) = (5 - 13) \bmod 26 = -8 \bmod 26 = 18 = S$
G = 6, $E(6) = (6 - 13) \bmod 26 = -7 \bmod 26 = 19 = T$
U = 20, $E(20) = (20 - 13) \bmod 26 = 7 \bmod 26 = 7 = H$
N = 13, $E(13) = (13 - 13) \bmod 26 = 0 \bmod 26 = 0 = A$
P = 15, $E(15) = (15 - 13) \bmod 26 = 2 \bmod 26 = 2 = C$
R = 17, $E(17) = (17 - 13) \bmod 26 = 4 \bmod 26 = 4 = E$
C = 2, $E(2) = (2 - 13) \bmod 26 = -11 \bmod 26 = 15 = P$

Ciphertext = IFESTHACEP

2. Soal No-2 : Buat satu kalimat sederhana (min 3 kata & total min 15 huruf), enkripsikan dengan Affine Cipher dan kembalikan menjadi plainteks

Plaintext = THE FLOWERS OF EVIL, $a = 5$, $b = 10$

T = 19, $E_k(19) = (5 * 19 + 10) \bmod 26 = 105 \bmod 26 = 1 = B$
H = 7, $E_k(7) = (5 * 7 + 10) \bmod 26 = 45 \bmod 26 = 19 = T$
E = 4, $E_k(4) = (5 * 4 + 10) \bmod 26 = 30 \bmod 26 = 4 = E$
F = 5, $E_k(5) = (5 * 5 + 10) \bmod 26 = 35 \bmod 26 = 9 = J$
L = 11, $E_k(11) = (5 * 11 + 10) \bmod 26 = 65 \bmod 26 = 13 = N$
O = 14, $E_k(14) = (5 * 14 + 10) \bmod 26 = 80 \bmod 26 = 2 = C$
W = 22, $E_k(22) = (5 * 22 + 10) \bmod 26 = 120 \bmod 26 = 16 = Q$
E = 4, $E_k(4) = (5 * 4 + 10) \bmod 26 = 30 \bmod 26 = 4 = E$
R = 17, $E_k(17) = (5 * 17 + 10) \bmod 26 = 95 \bmod 26 = 17 = R$
S = 18, $E_k(18) = (5 * 18 + 10) \bmod 26 = 100 \bmod 26 = 22 = W$
O = 14, $E_k(14) = (5 * 14 + 10) \bmod 26 = 80 \bmod 26 = 2 = C$
F = 5, $E_k(5) = (5 * 5 + 10) \bmod 26 = 35 \bmod 26 = 9 = J$
E = 4, $E_k(4) = (5 * 4 + 10) \bmod 26 = 30 \bmod 26 = 4 = E$
V = 21, $E_k(21) = (5 * 21 + 10) \bmod 26 = 115 \bmod 26 = 11 = L$
I = 8, $E_k(8) = (5 * 8 + 10) \bmod 26 = 50 \bmod 26 = 24 = Y$
L = 11, $E_k(11) = (5 * 11 + 10) \bmod 26 = 65 \bmod 26 = 13 = N$

$$a^{-1} = \text{GCD}(5, 26)$$

$$26 = 5 * 5 + 1$$

$$25 = 1 * 25 + 0$$

$$t_0 = 0, t_1 = 1$$

$$t_2 = (t_0 - (q_1 * t_1)) \bmod 26 = (0 - (5 * 1)) \bmod 26 = -5 \bmod 26 = 21 = a^{-1}$$

Ciphertext = BTE JNCQERW CJ ELYN

$B = 1, D_k(1) = 21 * (1 - 10) \bmod 26 = -189 \bmod 26 = 19 = T$

$T = 19, D_k(19) = 21 * (19 - 10) \bmod 26 = 189 \bmod 26 = 7 = H$

$E = 4, D_k(4) = 21 * (4 - 10) \bmod 26 = -126 \bmod 26 = 4 = E$

$J = 9, D_k(9) = 21 * (9 - 10) \bmod 26 = -21 \bmod 26 = 5 = F$

$N = 13, D_k(13) = 21 * (13 - 10) \bmod 26 = 63 \bmod 26 = 11 = L$

$C = 2, D_k(2) = 21 * (2 - 10) \bmod 26 = -168 \bmod 26 = 14 = O$

$Q = 16, D_k(16) = 21 * (16 - 10) \bmod 26 = 126 \bmod 26 = 22 = W$

$E = 4, D_k(4) = 21 * (4 - 10) \bmod 26 = -126 \bmod 26 = 4 = E$

$R = 17, D_k(17) = 21 * (17 - 10) \bmod 26 = 147 \bmod 26 = 17 = R$

$W = 22, D_k(22) = 21 * (22 - 10) \bmod 26 = 252 \bmod 26 = 18 = S$

$C = 2, D_k(2) = 21 * (2 - 10) \bmod 26 = -168 \bmod 26 = 14 = O$

$J = 9, D_k(9) = 21 * (9 - 10) \bmod 26 = -21 \bmod 26 = 5 = F$

$E = 4, D_k(4) = 21 * (4 - 10) \bmod 26 = -126 \bmod 26 = 4 = E$

$L = 11, D_k(11) = 21 * (11 - 10) \bmod 26 = 21 \bmod 26 = 21 = V$

$Y = 24, D_k(24) = 21 * (24 - 10) \bmod 26 = 294 \bmod 26 = 8 = I$

$N = 13, D_k(13) = 21 * (13 - 10) \bmod 26 = 63 \bmod 26 = 11 = L$

Plaintext = THE FLOWERS OF EVIL