Ahmad Irfan Fadholi
140810180034

Exercise Shift Cipher

1. Enkripsi ECLIPSE, K=18
   E(4) = (4+18) mod 26 = 22 mod 26 = 22 => W
   E(2) = (2+18) mod 26 = 20 mod 26 = 20 => U
   E(11)=(11+18) mod 26 = 29 mod 26 = 3 => D
   E(8)=(8+18) mod 26 = 26 mod 26 = 0 => A
   E(15)=(15+18) mod 26 = 33 mod 26 = 7 => H
   E(18)=(18+18) mod 26 = 36 mod 26 = 10 => K
   E(4) = (4+18) mod 26 = 22 mod 26 = 22 => W
   Hasilnya :
   WUDAHKW
2. Dekripsi WYHRRYPWAVRLYLUQVD, K=7
   D(22)=(22-7) mod 26 = 15 mod 26 = 15 => P
   D(24)=(24-7) mod 26 = 17 mod 26 = 17 => R
   D(7)=(7-7) mod 26 = 0 mod 26 = 0 => A
   D(17)=(17-7) mod 26 = 10 mod 26 = 10 => K
   D(17)=(17-7) mod 26 = 10 mod 26 = 10 => K
   D(24)=(24-7) mod 26 = 17 mod 26 = 17 => R
   D(15)=(15-7) mod 26 = 8 mod 26 = 8 => I
   D(22)=(22-7) mod 26 = 15 mod 26 = 15 => P
   D(0)=(0-7) mod 26 = -7 mod 26 = 19 => T
   D(21)=(21-7) mod 26 = 14 mod 26 =>O
   D(17)=(17-7) mod 26 = 10 mod 26 = 10 => K
   D(11)=(11-7) mod 26 = 4 mod 26 = 4 => E
   D(24)=(24-7) mod 26 = 17 mod 26 = 17 => R
   D(11)=(11-7) mod 26 = 4 mod 26 = 4 => E
   D(20)=(20-7) mod 26 = 13 mod 26 = 13 => N
   D(16)=(16-7) mod 26 = 9 mod 26 = 9 => J
   D(21)=(21-7) mod 26 = 14 mod 26 => O
   D(3)=(3-7) mod 26 = -4 mod 26 = 22 => W
   Hasilnya :
   PRAKKRIPTOKERENJOW

Exercise ROT 13

1. VSRFGUNPRC, K=13
   D(21) = (21-13) mod 26 = 8 mod 26 = 8 => I
   D(18) = (18-13) mod 26 = 5 mod 26 = 5 => F
   D(17) = (17-13) mod 26 = 4 mod 26 = 4 => E
   D(5) =(5-13) mod 26 = -8 mod 26 = 18 => S
   D(6) = (6-13) mod 26 = -7 mod 26 = 19 => T
   D(20) = (20-13) mod 26 = 7 mod 26 = 7 => H
   D(13) = (13-13) mod 26 = 0 mod 26 = 0 => A
   D(15) = (15-13) mod 26 = 2 mod 26 = 2 => C
   D(17) = (17-13) mod 26 = 4 mod 26 = 4 => E
   D(2) = (2-13) mod 26 = -11 mod 26 = 15 => P
   Hasilnya :
   IFESTHACEP

Tugas :
Buat satu kalimat sederhana (min 3 kata & total min 15 huruf), enkripsikan dengan Affine Cipher dan kembalikan menjadi plainteks :
AHMAD IRFAN FADHOLI, a = 7, b = 3
Enkripsi
E(0) = (0(7) + 3) mod 26 = 3 mod 26 = 3 => D
E(7) = (7(7) + 3) mod 26 = 26 mod 26 = 0 => A
E(12) = (12(7) + 3) mod 26 = 87 mod 26 = 9 => J
E(0) = (0(7) + 3) mod 26 = 3 mod 26 = 3 => D
E(3) = (3(7) + 3) mod 26 = 24 mod 26 = 24 => Y

E(8) = (8(7) + 3) mod 26 = 59 mod 26 = 7 => H
E(17) = (17(7) + 3) mod 26 = 122 mod 26 = 18 => S
E(5) = (5(7) + 3) mod 26 = 38 mod 26 = 12 => M
E(0) = (0(7) + 3) mod 26 = 3 mod 26 = 3 => D
E(13) =(13(7) + 3) mod 26 = 94 mod 26 = 16 => Q

E(5) = (5(7) + 3) mod 26 = 38 mod 26 = 12 => M
E(0) = (0(7) + 3) mod 26 = 3 mod 26 = 3 => D
E(3) = (3(7) + 3) mod 26 = 24 mod 26 = 24 => Y
E(7) = (7(7) + 3) mod 26 = 26 mod 26 = 0 => A
E(14) = (14(7) + 3) mod 26 = 101 mod 26 = 23 => X
E(11) = (11(7) + 3) mod 26 = 80 mod 26 = 2 => C
E(8) = (8(7) + 3) mod 26 = 59 mod 26 = 7 => H
Hasilnya :
DAJDY HSMDQ MDYAXCH

Dekripsi
GCD(7,26)
26 = 7 * 3 + 5
7 = 5 * 1 + 2
5 = 2 * 2 + 1
2 = 1 * 2 + 0
t0 = 0, t1 = 1
t2 = (t0 - (q1*t1)) mod 26 = (0 - (3*1)) mod 26 = -3 mod 26 = 23
t3 = (t1 - (q2*t2)) mod 26 = (1 - (1*23)) mod 26 = -22 mod 26 = 4
t4 = (t2 - (q3*t3)) mod 26 = (23 - (2*4)) mod 26 = 15 mod 26 = 15
a^{-1} = 15
D(3) = 15(3-3) mod 26 = 0 mod 26 = 0 => A
D(0) = 15(0-3) mod 26 = -45 mod 26 = 7 => H
D(9) = 15(9-3) mod 26 = 90 mod 26 = 12 => M
D(3) = 15(3-3) mod 26 = 0 mod 26 = 0 => A
D(24) = 15(24-3) mod 26 = 315 mod 26 = 3 => D

D(7) = 15(7-3) mod 26 = 60 mod 26 = 8 => I
D(18) = 15(18-3) mod 26 = 225 mod 26 = 17 => R
D(12) = 15(12-3) mod 26 = 135 mod 26 = 5 => F
D(3) = 15(3-3) mod 26 = 0 mod 26 = 0 => A
D(16) = 15(16-3) mod 26 = 195 mod 26 = 13 => N

D(12) = 15(12-3) mod 26 = 135 mod 26 = 5 => F
D(3) = 15(3-3) mod 26 = 0 mod 26 = 0 => A
D(24) = 15(24-3) mod 26 = 315 mod 26 = 3 => D
D(0) = 15(0-3) mod 26 = -45 mod 26 = 7 => H
D(23) = 15(23-3) mod 26 = 300 mod 26 14 => O
D(2) = 15(2-3) mod 26 = -15 mod 26 11 => L
D(7) = 15(7-3) mod 26 = 60 mod 26 = 8 => I
Hasilnya :
AHMAD IRFAN FADHOLI