Nama : Yulia Citra
Nim : E1E120023

1. Algoritma : KSA
Plaintext : 2107 → pakai nim E1E120023
kunci : saputra 1 - Len (K) = 8
Array : [0, 1, 2, 3 .... 100, 101, ... 254, 255]

tentukan key pakai desimal

K0 → s = 115		K4 → t = 116	
K1 → a = 97		K5 → r = 114	
K2 → P = 112		K6 → a = 97	
K3 → u = 117		K7 → 1 = 49	

→ literasi pertama i = 0
j = 0
j = [j + s (i)] + k [i mod len (K)] mod 256
= [0 + 0 + K [0 mod 8] Mod 256
= [K [0]] mod 256
= K0 → s = 115 → desimal
= 115 mod 256
j = 115
swap = (s [i], s [j]), → [s [j], s [i])
swap = (s [0], s [115]), → [s [115], s [0])
Array s = [115 - 1, 2, 3 .... , 114, 0, 116 .... 254, 255]
→ literasi kedua i = 1
j = 115
j = [j + s [i] + k [1 mod length (K)]] mod 256
= [115 + s [1] + K [1 mod 8]] mod 256
= [115 + 1 + K [1] mod 256
= [116 + K1/a] mod 256
= [116 + 97] mod 256
= 213 mod 256
j = 213
swap = (s [i], s [j]) = (s [j], s [i])
swap = (1, 213) = (213, 1)
Array s = [115, 213, 2, 3, ... 114, 0, 116, ... 212, 1, 214 ... 254, 255)
⇒ Literasi ketiga i = 2
j = 213

j = (j + s[i] + k[i mod length(k)]) mod 256
= (213 + s[2] + k[2 mod 8]) mod 256
= (213 + 2 + k[2] mod 256
= (215 + K_2 /P) mod 256
= (215 + 112) mod 256
= 327 mod 256
j = 71
swap = (s[i], s[j]) = (s[i])
swap = (s[2], s[71]) = (s[71], s[i])
Array s = [115, 213, 71, 3, 4, 5 .... 70, 2, 72, 73, ... 114, 0, 116 ... 212, 1, 214 ... 254, 256]
⇒ Literasi ke empat i = 3
j = 71
j = [j + s[i] + k[i mod length(k)]] mod 256
= [71 + s[3] + k[3 mod 8]] mod 256
= [71 + 3 + k[3] mod 256
= [74 + K_3 /u) mod 256
= [74 + 117] mod 256
j = 191 mod 256
j = 191
swap = [s[i], s[j]) = (s[j], s[i])
swap = (s[3], s[191] = (s[191], s[3])
Array s = (115, 213, 71, 191, 4, 5 .... 70, 2, 72, 73 ... 114, 0, 116 .. 190, 3, 192 ... 212 .. 1
214 ... 254, 255)
⇒ Literasi ke lima i = 4
j = 191
j = [j + s[i] + k[i mod length(k)) mod 256
= [191 + s[4] + k[4 mod 8) mod 256
= (191 + 4 + k[43] mod 256
= (195 + K_4 /+) mod 256
= (195 + 116) mod 256
= 311 mod 256
j = 55
swap = (s[i], s[j]) = (s[j], s[i])
swap = (s[4], s[55]) = (s[55], s[4])
Array s = [115, 213, 71, 191, 55, 5, 6, 7, 8 ... 54, 4, 55, 70, 2, 114, 0, 116 ...
190, 3, 192, ... 212, 1, 214 ... 254, 255)

→ Literasi ke enam i = 5

j = 55

j = (j + s[i] + k[i mod length(k)]) mod 256

= (55 + s[5] + k[5 mod 8]) mod 256

= (60 + k[5]) mod 256

= (60 + k2 / r) mod 256

= (60 + 114) mod 256

= 174 mod 256

j = 174

Swap = (s[i], s[j]) = (s[j], s[i])

swap = (s[5], s[174]) = (s[174], s[5])

Array s = [115, 213, 71, 191, 55, 174, 6, 7, 8 ... 54, 4, 56 ... 70, 2, 72 ... 114, 0, 116 ... 173, 5, 175 ... 190, 3, 192 ... 212, 1, 214 ... 254, 255]

→ Literasi ke tujuh i = 6

j = 174

j = [j + s[i] + k[i mod length(k)] mod 256

= (174 + s(6) + k[6 mod 8]) mod 256

= (174 + 6 + k[6]) mod 256

= (180 + k6 / a) mod 256

= (180 + 97) mod 256

= 277 mod 256

j = 21

Swap = (s[i], s[j]) = (s[j], s[i])

swap = (s(6), s[21]) = (s[21], s[6])

Array s = [115, 213, 71, 191, 55, 179, 21, 7, 0 ... 20, 6, 22 ... 54, 4, 56, ... 70, 2, 72 ... 114, 0, 116 ... 176, 5, 175 ... 190, 3, 192 ... 212, 1, 214 ... 254, 255]

→ Literasi ke delapan i = 7

j = 21

j = [j + [i] + k[i mod length[k]] mod 256

= (21 + s[7] + k[7 mod 8]) mod 256

= (21 + 7 + k[7] mod

= (28 + k[7] mod 256

= (28 + k, 11) mod 256

= (28 + 49) mod 256

= 77 mod 256

j = 77

Swap = (s[i], s[j]) = (s[j], s[i])

swap = (s[7], s[77]) = (s[77], s[7])

Array S = (115, 213, 71, 191, 55, 174, 21, 77, 8, 19, 20, 6, 22 ... 54, 4, 56 ..
70, 2, 72, 73, 74, 75, 76, 7, 78 ... 114, 0, 116, ... 173, 5, 175 ... 1
3, 192 ... 212, 1, 214, 254, 255)

2. PRGA

NIM = E1E1 20023

P = 2023

Arrays = [115, 213, 71, 191, 55, 174, 21, 77, 8, 9 ....., 19, 20, 6, 22, ..., 54, 4,
70, 2, 72, 73, ..., 76, 7, 78, ..., 113, 114, 0, 116, ..., 173, 5, 175, ...
190, 3, 192, ..., 212, 1, 214, ..., 254, 255]

→ Iterasi pertama

J = 0 i = 0

i = (i + 1) mod 256
= (0 + 1) mod 256
= 1 mod 256
i = 1

j = (j + S[i]) mod 256
= (0 + S(1)) mod 256
= (0 + 213) mod 256
j = 213

Swap (S(i), S(j)) → S(1) ⇄ S(213)

t = (S(i) + S(j)) mod 256
= (S(213) + S(1)) mod 256
= (213 + 1) mod 256
t = 214

U = S(t) → S(214)

e = U ⊕ P[0]
= 214 ⊕ 2
= 11010110 // Ubah ke biner
00000010 ⊕ // ubah ke decimal
11010100 → 212 = Ô // Ubah ke Character

→ Iterasi kedua

j = 213 i = 1

i = (i + 1) mod 256
= (1 + 1) mod 256
= 2 mod 256
i = 2

J = (J + S(i)) mod 256
= (213 + S(2)) mod 256
= (213 + 71) mod 256
= 284 mod 256
j = 28

Swap (S(i), S(j)) → S(2) ⇄ S(28)

t = (S(i) + S(j)) mod 256

= (S(28) + S(2)) mod 256

= (71 + 28) mod 256

t = 99

u = S(t) → S(99)

c = u ⊕ P[1]

= 99 ⊕ 0

= 01100011 // ubah ke biner

00000000 ⊕ // ubah ke decimal

01100011 → 99 = c // Ubah ke Character

→ Iterasi ketiga

j = 28 i = 2

i = (i + 1) mod 256

= (2 + 1) mod 256

i = 3

j = (j + S(i)) mod 256

= (28 + S(3)) mod 256

= (28 + 191) mod 256

j = 219

Swap (S(i), S(j)) → S(3) ⇄ S(219)

t = (S(i) + S(j)) mod 256

= (S(219) + S(3)) mod 256

= (219 + 191) mod 256

t = 154

u = S(t) → S(154)

No:

C = U ⊕ P[2]

= 154 ⊕ 2

= 10011010 // ubah ke biner

00000010 ⊕ // ubah ke decimal

10011000 → 152 = ~ // Ubah ke character

→ Iterasi keempat

j = 219 i = 3

i = (i + 1) mod 256

= (1 + 3) mod 256

i = 4

j = (j + S(i)) mod 256

= (219 + S(4)) mod 256

= (219 + 55) mod 256

= 274 mod 256

j = 18

swap (S(i), S(j)) → S(4) ⇄ S(18)

t = (S(i) + S(j)) mod 256

= (S(18) + S(4)) mod 256

= (55 + 18) mod 256

t = 73

u = S(t) → S(73)

c = u ⊕ P[3]

= 73 ⊕ 3

= 01001001 // ubah ke biner

00000011 ⊕ // ubah ke decimal

01001010 → 74 = J // Ubah ke character