Nama : Deni Hidayat
Nim : E1E120026
Matkul : Kriptografi

Soal

1. Kerjakan KSA dan PRGA dengan prosedur dan dgn kunci Saputra 1.

Jawab :

Array S = [0,1,2,3,4,5,6,7,8,9,10,11,.....,56,57,58,.....,
250,251,252,253,254,255,256]

Dik :
K : Saputra 1 length = 8
$k_0$ : S = 115
$k_1$ : a = 97
$k_2$ : p
$k_3$ : u
$k_4$ : t
$k_5$ : r
$k_6$ : a
$k_7$ : 1

J = 0 J = 0 (i pertama)
J = (J + S[i] + k[i mod length(k)]) mod 256
J(0) = (0 + S(0) + k(0 mod length(8))) mod 256
= (0 + 0 + k[5]) mod 256
= (0 + k[115]) mod 256
= 115 mod 256
Swap = (S[i], S[J])
Swap = (S[0], S[115])
S = [115,1,2,3,4,5,6,7,8,9,10,.....,56,57,58,115,114,0,116,17,...
253,254,255,256]

* i = 1, j = 115

j = (j + S[i] + k[i % Length(k)]) % 256

= (115 + 1 + k[1 % 8]) % 256

= (115 + 1 + 97) % 256

= 213 % 256

= 213

Swap (S[1], S[213])

S = [115, 213, 3, 3, 4, 5, 6, 7, ····, 209, 210, 211, 212, 1, 214, ··256]

* i = 2, j = 213

j = (j + S[i] + k[i % Length(k)]) % 256

= (213 + S[2] + k[2 % 8]) % 256

= (213 + 2 + 112) % 256

= 327 % 256

= 71

Swap (S[2], S[71])

S = 115, 213, 71, 3, 4, 5, 6, 7, ···· 69, 70, 2, 72, 73, ···· 255, 256]

* i = 3, j = 71

j = (j + S[i] + k[i % Length(k)]) % 256

= (71 + S[3] + k[3 % 8]) % 256

= (71 + 3 + 117) % 256

= 191 % 256

= 191

Swap (S[3], S[191])

S = [115, 213, 71, 191, 4, 5, 6, ····, 189, 190, 3, 192, ··· 255, 256]

* i = 4, j = 191

j = (j + S[i] + k[i % Length(k)]) % 256

= (191 + S[4] + k[4 % 8]) % 256

= (191 + 4 + 116) % 256

= 311 % 256

= 55

swap (S[4], S[55])

S = [115, 213, 71, 191, 55, 5, 6, ···, 50, 51, 52, 53, 54, 4, 56, ··256]

No.

Date :

* i = 5 , j = 55

j = (j + S[i] + K[i % length(k)]) % 256

= (55 + S[5] + K[5 % 8]) % 256

= (55 + 5 + 114) % 256

= 174 % 256

= 174

swap (S[5], S[174])

S = [115, 213, 71, 191, 55, 174, 6, 7, ···, 173, 5, 175, 176, ··, 256]

* i = 6 , j = 174

j = (j + S[i] + K[i % length(k)]) % 256

= (174 + S[6] + K[6 % 8]) % 256

= (174 + 6 + 97) % 256

= (277) % 256

= 21

swap (S[6], S[21])

S = [115, 213, 71, 191, 55, 174, 21, 7, 8, ···, 20, 6, 22, ···, 255, 256]

* i = 7 , j = 21

j = (j + S[i] + K[i % length(k)]) % 256

= (21 + S[7] + K[7 % 8]) % 256

= (21 + 7 + 49) % 256

= 77 % 256

= 77

swap (S[7], S[77])

S = [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, ···, 73, 74, 75, 76, 7, 78, ···
255, 256]

2. Kerjakan PRGA dengan plaintext nim dan kunci saputra1 !

Jawab

- plaintext = 2026
- kunci = saputra1
- S = [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, ... 258, 254, 255]

```
i = 0
j = 0
for idx = 0 to length (p) - 1 :
        i = (i+1) % 256
        j = (j+S[i] % 256
        Swap (S[i], S[j])
        t = (S[i] + S[j] mod 256
        u = S(t)
        c = u ⊕ P(idx)
end
```

* i = 0 j = 0

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

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

Swap (S[i], S[j])
Swap (S[1], S[213])

t = (S[i] + S[j] % 256
= (S[213] + S[1] % 256
= (213 + 1) % 256
= 214

u = S(t)
= S(214)

c = u ⊕ P(0) = 214 ⊕ 2
= 11010110
00000010 ⊕
11010100 → P 212 → chr 0

No.

Date :

* i = 1 , j = 213

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

j = (j + s[i] % 256
= (213 + S[2]) % 256
= (213 + 71) % 256
= 284 % 256 = 28

swap (s[i], s[j])
swap (S[2], s[28])

t = (s[i] + s[j] % 256
= (S[28] + S[2] % 256
= (71 + 28] % 256
= 99 % 256
= 99

u = S[t]
= s[99]

C = U ⊕ P[1]
= 99 ⊕ P[1]
= 9 ⊕ 0
= 0 1 1 0 0 0 1 1

0 0 0 0 0 0 0 0 ⊕
0 1 1 0 0 0 1 1 → 99 = "C"

* i = 2 , j = 28

i = (i+1) % 256
= (2+1) % 256
= 3

j = (j + s[i]) % 256
= (28 + S[3] % 256
= (28 + 191) % 256
= 219

swap (s[i], s[j])
swap (S[3], s[219])

t = (s[i] + s[j] % 256
= (S[219] + S[3]) % 256
= (219 + 191) % 256
= 410 % 256
= 154

u = S[t]
= S[154

C = U ⊕ P[2]
= 159 ⊕ 2
= 1 0 0 1 1 0 1 0

0 0 0 0 0 0 1 0 ⊕
1 0 0 1 1 0 0 0 → 152 = "ไ"