No.

Date . .

Nama : Muh. Abdillah
Nim = E1E120080
Kelas = Genap
Mata kuliah = kriptografi

0 KSA (Key Scheduling Algorithm)

inisialisasi = $S_0 = S_1 \cdots S_{255} = 255$

key : Saputra1 → length key = 8

Iterasi ke-0

i = 0 J = 0 S = 115

J = (J + S[i] + K[i mod len(k)]) mod 256

= (0 + 0 + K[0 mod 8]) mod 256

= (0 + K[0]) mod 256

= (0 + 115) mod 256

= 115 mod 256

J = 115

swap = S[i] S[J] = S[0], S[115]

S = 115, 2, 3, 4, 5, 6, 7 ..., 114, 0, 116 .. 255

Iterasi ke-1

i = 1 J = 115 a = 97

J = (J + S[i] + K[i mod len(K)]) mod 256

= (115 + 1 + K[1 mod 8]) mod 256

= (116 + [illegible]) mod 256

= (116 + 97) mod 256

= 213 mod 256

J = 213

No.

Date . .

swap = S[i], S[j] = S[1] S[213]

S = 115, 213, 3, 4, 5 ..., 114, 0, 116 ... 212, 1, 214 ... 255

Iterasi ke 2

i = 2 J = 213 P = 112

J = (J + S(i) + K[i mod len(K) J) mod 256

= (213 + 2 + K[2 mod 8]) mod 256

= (215 + K[2]) mod 256

= (215 + 112) mod 256

= (327 mod 256)

J = 71

swap = S[i], S[j] = S[2], S[71]

Iterasi ke - 3

i = 3 J = 71 K = 117

J = [J + S(i) + K[i mod len(K) J) mod 256

= (71 + 3 + K (3 mod 8)) mod 256

= (74 + K(3)) mod 256

= 191 mod 256

J = 191

swap = S(i), S(J) = S(3) S(191)

S = 115, 213, 71, 191, 55, 5 ... 54, 4, 56, ... 70, 72, 119,

0, 116, ..., 190, 3, 192, ..., 212, 1, 214, ... 255

No.

Date . .

Herasi ke-5

i = 5 J = 55 S = 119

J = (J + S(i) + K(i mod len(K)) J) mod 256

= (55 + 5 + K(5 mod 8)) mod 256

= (60 + K(5)) mod 256

= (60 + 119) mod 256

= 174 mod 256

J = 174

swap = S(i), S(J) = S(5), S(174)

S = 115, 213, 71, 191, 55, 174, 6, ..., 54, 4, 56, ...,
70, 2, 72, ..., 114, 0, 116, ..., 190, 3, 192, ..., 252,
1, 214, ..., 255

Herasi ke 6

i = 6 J = 174 a = 97

J = (J + S(i) + K(i mod len(K)) J) mod 256

= (174 + 6 + K(6 mod 8)) mod 256

= (180 + K(6)) mod 256

= (180 + 97) mod 256

= 277 mod 256

J = 21

swap = S(i), S(J) = S(6), S(21)

S = 115, 213, 71, 191, 55, 174, 21, 7, ..., 20, 6, 22,
..., 54, 4, 56, ... 70, 2, 72, ..., 114, 0, 116,
..., 173, 5, 190, ..., 190, 3, 192, ..., 212,
1, 214, ..., 255

Iterasi ke 7

i = 7 j = 21 1 = 49

j = [j + s(i) + k(i mod (len(k))) mod 256

= (21 + 7 + k(7 mod 8)) mod 256

= (28 + k(7)) mod 256

= (28 + 49) mod 256

= 77 mod 256

j = 77

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

s = 115, 243, 71, 192, 55, 174, 21, 77, 8, ...,
20, 6, 22, ..., 54, 19, 56, ..., 70, 2, 72, ...,
76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ...,
190, 3, 192, ..., 202, 1, 214, ..., 255

No.

Date . .

Nama = Muh. Abdillah
Nim = E1E1 20080
Kelas = Genap
Mata kuliah = Kriptografi

Pseudo Random Generation Algorithm (PRGA)
Plaintek = 2008q

- Harap pertama

i = 0 j = 0

For idx = 0 to length (P) - 1 do
= 0 to len (J) - 1 do
= 0 to 4 do

$i = (i + 1) \bmod 256$
$i = (0 + 1) \bmod 256$
$i = 1$
$j = (j + S(i)) \bmod 256$
$j = (0 + 243) \bmod 256$ // nilai i diambil dari array sebelumnya di KSA

swap = S(i), S(j) = S(1), S(243)

$t = (S(1) + S(j)) \bmod 256$
u = S(t)
$= (1 + 243) \bmod 256$
$= 244 \bmod 256$
t = 244
= S(244)

C = u ⊕ P(6)
= 244 ⊕ 2

No.

Date . .

⇒ Binary = 0214 ⇒ 11010110

2 ⇒ 00110010 ⊕ xOR

11100100 → 228 ⇒ ä

- Harcfi ke 2

I = 1 , J = 213

for index = 0 to 9

i = (i + 1) mod 256

I = (1 + 1) mod 256

= 2 mod 256

= 2

J = (S(I), S(J)) mod 256

= (213 + 3(2)) mod 256

= (213 + 71) mod 256

= 284 mod 256

= 99

C = U ⊕ P(1)

= 99 ⊕ 0

⇒ 01100011

01110000 ⊕

01010011 → chr ⇒ S (kapital)

No.

Date . .

- Harapi Ice 3

$i = 2 \quad j = 28$

For idx = 0 to 4 do

$i = (2+1) \bmod 256$

$i = 3 \bmod 256$

$i = 3$

$J = (J + S(i)) \bmod 256$

$= (28 + 191) \bmod 256$

$= 219 \bmod 256$

$J = 219$

swap $= S(1), S(J) = S(3), S(219)$

$t = (S(3) + S(219)) \bmod 256$

$= (219 + 191) \bmod 256$

$= 410 \bmod 256$

$= 154$

$u = S(154)$

$C = u \oplus P(2)$

$= 54 \oplus 0$

$= 10011010$

00110000

10101010

Dec = 170

ASCII = a

No.

Date . .

- Huruf ke 4

i = 3 j = 219

for idx = 0 to 4 do

i = (3+1) mod 256

= 4

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

= (219 + 55) mod 256

= 274 mod 256

j = 18

swap : s(i) s(j) = s(4) s(18)

t = (s(4) + s(18)) mod 256

= (18 + 55) mod 256

= 73

u = s(73)

c = u ⊕ p(3)

= 73 ⊕ 8

Binary = 0 1 0 0 1 0 0 1

0 0 1 1 1 0 0 0 ⊕ Dec : 113 ascii = q

0 1 1 1 0 0 0 1

No.

Date . .

- Heraft 5

i = 4 j = 19

for idx = 0 to 4 do

= (4 + 1) mod 256

= 5

j = (181 + 174) mod 256

= 192 mod 256 ⇒ j = 192

swap = S(i), S(j) = S(115), S(192)

t = (192 + 174) mod 256

= (366) mod 256

t = 110

u = S(110)

c = u ⊕ P(9)

= 110 ⊕ 0

Binary = 01101110

00110000 ⊕

01011110

Des = 94

Ascii = ^