Nama : Rizky Prasetya Ardana
kelas : Ganjil
NIM : E1E1 20 091

Algoritma key Scheduling Algoritma (KSA)

kunci : "Saputra", len(k) = 8
Array s : [0,1,2,3,4,5,6,7,8,....,100,101,102,103,....,253,254,255]

*Iterasi Pertama → i = 0
j = 0
*j = (j + S[i] + K[i mod len(k)] mod 256
= (0 + 0 + K[0 % 8]) % 256
= (K[0]) % 256
= ("S") % 256 ⇒ nilai desimal dari "s" . 115
= 115 % 256
j = 115
Swap (S[i], S[j])
Swap (S[0], S[115])
Array S . [115,1,2,3,4,5,6,7,....110,111,112,113,114,0,116,117,....
199,200,201,202,203,204,205, ... 250,251,252,253
254,253]

*Iterasi kedua → i = 1
j = 115
*j = (j + S[i] + K[i% len(k)]) % 256
= (115 + S[i] + k[1% 8]) % 256
= (115 + 1 + k[i]) % 256
= (116 + "a") % 256 desimal dari "a" = 97
= (116 + 97) % 256
= 213 % 256
j = 213
Swap (S[i] . S[j])
swap (S[i] . S[213])
Array S = [115,213,2,3,4,5,6,7,....,112,113,114,0,116,...
210,211,212,1,214 .... 250,251,252,253,254,255]

* Iterasi ketiga → i=2

j =213

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

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

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

=(215 + "p") % 256 => desimal dari *p* =112

=(215 +112) % 256

= 327 % 256

j = 71

swap (S[i] , S[j])

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

Array S =[115,213,71,3,4,5,6,7,....69,70,2,72....
112,113,114,0,116,....210,211,212,1,2,4....
250,251,252,253,254,255]

* Iterasi keempat → i =3

j =71

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

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

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

= (74 + (17) % 256

= 191 % 256

j =191

swap(S[i], S[j])

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

Array S = [115,213,71,191,4,5,6,7,....,69,70,2,72,...
112,113,114,0,116, ...,189,190, 3,192,.... 210,
211,212,1,214 250,251,252,253,254,
255]

*Iterasi kelima

i =4, j =191
j :(j + S[i] + k [i mod length(k)] mod 256
j =(191 +4 + k [4 mod (8)]) mod 256
j = (195 + k4) mod 256
j =(195 + 116) mod 256 = 311 mod 256
j= 55
Swap(S[i], S[i])
Swap (S[4], S[55])
Array s =[115, 213 71, 191, 55, 5, ... 53, 54, 4, 56, ..., 70, 2, 72, ... 114, 0, 116, ... 190, 3, 192, ... 212, 1, 214, ..., 253, 254, 255]

*Iterasi keenam

i =5, j =55
j =(j + S[i] + k[i mod length(k)]) mod 256
j =(55 + 5 + k[5 mod (8)]) mod 256
j =(60 + 114) mod 256
j = 174 mod 256
j = 174
Swap (S[i], S[i])
Swap (S[5], S [174])
Array s =[115, 213, 71, 191, 55, 174, 6, 7, 8, ..., 53, 54, 4, 56, ..., 70, 2, 72, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212, 1, 214, ..., 254, 255]

*Iterasi ketujuh

i = 6, j =174
j =(j + S[i] + k [i Mod length[k]) Mod 256
j =(174 + 6 + k[6 Mod (8)]) Mod 256
j =(180 + k6) Mod 256
j =(180 + 97) Mod 256
j = 277 Mod 256
j = 21

* Iterasi kedelapan

i = 7, j = 21

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

j = (21 + 7 + K (7 mod (8)]) mod 256

j = (28 + K7) mod 256

j = (28 + 49) mod 256

j = 77 mod 256

j = 77

swap (S[i], S[j])

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

Array S = [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, ..., 20, 6, 22, ..
54, 4, 56, ..., 70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 114, 0,
116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212, 1, 214, ...,
253, 254, 255]

No.

Date

Metode PRGA

•> P=2091
i=0
j=0

Iterasi pertama
for index =0 to length (P)-1
For index =0 to (4)-1
i = (0+1) mod 256
i = 1

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

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

t = S[213] + S[1]
t = 213 + 1
t = 214

u = S[214]

C = 214 ⊕ P [idx]
= 214 ⊕ P [0]
= 214 ⊕ 2
= 11010110
00110010
11100100 => 228 = 'a'

No.

Date . .

Iterasi Kedua

i = 1

j = 213

For index = 0 to length (P) - 1

= 0 to length (4) - 1

I = (1+1) mod 256

i = (i+1) mod 256

i = 2 mod 256

i = 2

J = (j + S [i]) mod 256 swap= S [i], S [j]

j = (213 + S[2]) mod 256 S [2], S [28]

j = (213+71) mod 256

j = 284 mod 256

J = 28

t = S[2] + S[28]) mod 256 ⇒ u = S [99]

t = [28 + 71]

= 99

c = u ⊕ P [i] 01100011

= 99 ⊕ 0 ⇒ 00110000 = 83 ⇒ S (capital s)

= 01010011

No.

Date

Iterasi ketiga

i = 2, J = 28

For index . 0 to (3)

I = (i + 1) mod 256

i = (2+1) mod 256

i = (3) mod 256

i = 3

j = (j + s [i] mod 256

swap = (s [3] , s [219])

j = (28 + s [3] Mod 256

j = (28+191) mod 256

j = (219) mod 256

t = (S[3] + s [219]) mod 256

t = (219 + 191) Mod 256

t = (410) mod 256

t = 154

=> 4 = S [154]

C = 4 $\oplus$ P[2]

= 154 $\oplus$ 9

= 10011010

00111001

10100011

=> 163 = E

Iterasi Ke·Empat

i = 3, j = 219

For index = 0 to (8)

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

$i = (3 + 1) \bmod 256$

$i = 4$

$j = (j + S[i]) \bmod 256$

$j = (219 + 55) \bmod 256$

$j = (274) \bmod 256$

$j = 18$

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

(S[4], S[18])

$t = (S[4] + S[18])$

$= 18 + 55 \bmod 256$

$= 73$

u = 73

$C = u \oplus P[3]$

$= 73 \oplus 1$

$= 01001001$

$\underline{00110001} \oplus 120$ x

01111000

Hasilnya : "a" S E x