Nama : Raihan De Laindi
NIM : EIEI 20 090

- Algoritma : key - Scheduling Algorithm (KSA)

kunci : "Saputral" , 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

$j = 0$
$\Rightarrow j = (j + S[i] + k[i \text{ mod } len(k)]) \text{ mod } 256$
$= (0 + 0 + k[0 \% 8]) \% 256$
$= (k[0]) \% 256$
$= (\text{"s"}) \% 256$ ⇒ 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, ..., 250, 251, 252, 253, 254, 255]

- Iterasi kedua → i = 1

$j = 115$
$\Rightarrow j = (j + S[i] + k[i \% len(k)]) \% 256$
$= (115 + S[i] + k[i \% 8]) \% 256$
$= (115 + 1 + k[1]) \% 256$
$= (116 + \text{"a"}) \% 256$ ⇒ 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

$j = 213$
$\Rightarrow j = (j + S[i] + k[i \% len(k)]) \% 256$
$= (213 + S[i] + k[i \% 8]) \% 256$
$= (213 + 2 + k[3]) \% 256$
$= (215 + \text{"p"}) \% 256$ ⇒ 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 , 214 , ... , 230 , 251 , 252 , 253 , 254 , 255]

- Iterasi keempar → i = 3
  j = 71
  ⇒ j = (j + S [i] + u[i % len (u)]) % 256
  = (71 + S [3] + k[3 % 8]) % 256
  = (71 + 3 + k[3]) % 256
  = (74 + "u") % 256 ⇒ desimal dari "u" = 117
  = (74 + 117) % 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 , 235]

- Iterasi kelima → i = 4
  j = 191
  j = (j + S[i] + k [i % len (k)]) % 256
  = (191 + S[4] + u[4 % 8]) % 256
  = (191 + 4 + k [4]) % 256
  = (195 + "u") % 256 ⇒ desimal dari "u" = 116
  = (195 + 116) % 256
  = 311 % 256
  j = 55
  Swap (S [i] , S [j])
  Swap (S [4] , S [55])
  Array S = [115 , 213 , 71 , 191 , 55 , 5 , 6 , 7 , 8 , ... , 53 , 54 , 4 , 56 , 57 , ... , 69 , 70 , 2 , 72 , 73 , ...
  113 , 114 , 0 , 116 , 117 , ... , 189 , 190 , 3 , 192 , ... , 211 , 212 , 1 , 214 , ... , 250 , 251 , 252 ,
  253 , 254 , 255]

- Iterasi keenam → i = 5

j = 55

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

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

= (60 + "r") % 256 => desimal dari "r" = 119

= (60 + 114) % 256

= 174 % 256

= 174

Array s = [115, 213, 71, 191, 55, 174, 6, 7, 8, ···· , 53, 54, 4, 56, 57, ···· , 69, 70, 2, 72, 73, ···
113, 114, 0, 116, 117, ···· 172, 173, 5 , 175, 176, ···· , 189, 190, 3, 192, 193, ····
211, 212, 1, 214, 215, ···· , 250, 251, 252, 253, 254, 255]

- Iterasi ketujuh → i = 6

j = 174

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

= (174 + S [6] + k [6 % len (k)]) % 256

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

= (180 + "a") % 256 desimal dari "a" = 97

= (180 + 97) % 256

= 277 % 256

j = 21

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

Swap (S [6] , S [174])

Array S = [115, 213, 71, 191, 55, 174, 21, 7, 8, ···· , 19, 20, 6, 22, 23, ···· , 53, 54, 4,
56, 57, ···· , 69, 70, 2, 72, 73, ···· , 113, 114, 0, 116, 117, ···· , 172, 173, 5, 175, 176,
···· , 189, 190, 3, 192, 193, ···· , 211, 212, 1, 214 215, ···· , 250, 251, 252, 253,
254, 255]

- Iterasi ke delapan → i = 7

j = 21

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

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

= (28 + "1") % 256 desimal dari "1" = 49

= (28 + 49) % 256

= 77 % 256

j = 77

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

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

Array s = [115, 213, 74 191, 55, 21, 77, 8, ..., 19, 20, 6, 22, ..., 53, 54, 4, 56, ...
69, 70, 2, 72, 73, 74, 75, 76, 77, 78, ..., 113, 114, 0, 116, 117, ..., 172, 173, 5,
175, ..., 188, 190, 3, 192, 193, ..., 211, 212, 1, 214, 215, ... 250, 251, 252
253, 254, 255]

Algoritma : Pseudo-random Generation Algorithm (PRGA)

Array S : [115, 213, 71, 191, 55, 174, 21, 77, 8, ..., 19, 20, 6, 22, 23, ..., 53, 54, 4, 56, 57, ...
69, 70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 113, 114, 0, 116, 117, ..., 172, 173, 5, 175, 176, ...
189, 190, 3, 192, 193, ..., 211, 212, 1, 214, 215, ..., 250, 251, 252, 253, 254, 255

Plainteus : "2090"

- Iterasi: pertama → idx = 0

i = 0
j = 0

⇒ i = (i+1) % 256
= (0+1) % 256
= 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])

Array S = [115, 1, 71, 191, 55, 179, 21, 77, 8, ..., 19, 20, 6, 22, 23, ... 53, 54, 4, 56, 57, ...
69, 70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 113, 114, 0, 116, 117, ..., 172, 173, 5, 175, 176, ...
189, 190, 3, 192, 193, ..., 212, 213, 214, ..., 250, 251, 252, 253, 254, 255]

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

⇒ u = S[t]
= S[214] = 214 ⇒ biner 214 = 11010110

⇒ C = u ⊕ P[idx]
= u ⊕ P[0]
= u ⊕ "2" ⇒ biner "2" = 110010

= 11010110
00110010 ⊕
11100100

C = "a" didesimalkan menjadi 228

- Iterasi kedua → Idx = 1

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])

Array S = [115, 1, 28, 191, 55, 174, 21, 77, 8, ..., 19, 20, 6, 22, 23, ..., 26, 27, 71, 29, 30, ..., 53, 54, 4, 56, 57, ..., 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 113, 114, 0, 116, 117, ..., 172, 173, 5, 175, 176, 7..., 189, 190, 3, 192, 193, ..., 212, 213, 219, 215, ..., 250, 251, 252, 253, 254, 255]

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

⇒ u = S[t]
= S[99]
= 99 ⇒ biner 99 = 1100011

⇒ C = u ⊕ P (Idx)
= u ⊕ P[1]
= u ⊕ "0" ⇒ biner "0" = 110000

$$\begin{array}{r} 1100011 \\ 110000 \\ \hline 1010011 \end{array}$$

C = "S" desimal = 83

- Iterasi ketiga → Idx = 2

i = 2 , j = 28

⇒ i = (i + 1) % 256

= (2 + 1) % 256

= 3

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

Swap (S [3]), S[219])

Array S = [115, 1, 28, 219, 55, 174, 21. 77. 8. ⋯ , 19, 20, 6, 22, 23, ⋯ 26, 27, 71, 29. 30, – 53, 54. 4, 56, 57, ⋯ ,69, 70. 2, 72, 73. 74, 75. 76, 7. 78. 79, ⋯ ,113, 114. 0. 116, 117, ⋯ , 172, 173, 5, 175, 176, ⋯ , 189. 190, 3, 192, 193, ⋯ . 212. 213, 214, 215, 216, 217, 218, 191, 220, ⋯ , 253, 254, 255]

⇒ t = (S [i]) + (S [j]) % 256

= (S [3] + S [219]) % 256

= (219 + 191) % 256

= 410 % 256

= 154

⇒ u = S [t]

= S [154]

= 154 , biner 154 = 10011010

⇒ c = u ⊕ P [Idx]

= u ⊕ P [2]

= u ⊕ "g" ⇒ biner "g" = 111001

= 10011010

   111001

$$\begin{array}{r} 10011010 \\ 111001 \\ \hline 10100011 \end{array} \oplus$$

C = "£" decimal 163

- Iterasi ke empat => Idx = 3

i = 3 , j = 219

=> i = (i + 1) % 256
= (3 + 1) % 256
= 4

=> j = (j + S[i]) % 256
= (219 + S[4]) % 256
= (219 + 55) % 256
= 274 % 256
= 18

Swap (S[i] , S[j])
Swap (S[4] . S[18])

Array S = [115, 1, 28, 219, 18, 174, 21. 77, 8, ..., 16, 17, 55, 19, 20, 6, 22, 23, 24, 25, 26
27, 71, 29, 30, ..., 53, 54, 4, 56, 57, 69, 70, 21, 72, 73, 74, 75, 76, 7, 78, 79, ...
113, 114, 0, 116, 117, ..., 172, 173, 5, 175, 176, ..., 189; 190, 3, 192, 193, ..., 212,
213, 214, 215, 216, 217, 218, 191, 220, ..., 253, 254, 255]

=> t = (S[i] + S[J] % 256
= (S[4] + S[18] % 256
= 18 + 55 % 256
= 73

=> u = S[t]
= S[73]
= 73 => biner 73 = 1001001

=> c = u ⊕ P [idx]
= u ⊕ P [3]
= u ⊕ "0" => biner "0" : 110000

$$\begin{array}{r} 1001001 \\ 110000 \\ \hline 1111001 \end{array} \oplus$$

c = "y" desimal = 121