* Algoritma : Key - Scheduling Algoritma [KSA]

Kunci : Safitha 1 , len [k] = 8

Array S = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, . . ., 100, 101, 102, 103, . . .
253, 254, 255]

* Iterasi ~~[illegible]~~ 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

= 115 % 256

J = 115

Swap [S[i]], S[J]]

Swap [S[0],

117

Array S: [115, 1, 2, 3, 4, 5, 6, 7, . . ., 110, 111, 112, 113, 114, 0, 116, . . .,
~~246, 247, 248, +, 249, . . ., 250, 251, 252, 253, 254, 255~~].
199, 200, 201, 202, 203, 204, 205, . . ., 250, 251, 252, 253, 254, 255]

* iterasi kedua → i = 1

J = 115

→ J = [J + S[i] + k[i% len [k]]] % 256

~~= [115 + S[1] + k [1 % 8]~~

= [115 + S[1] + k [1 % 8]] % 256

= [115 + S[1] + k [1]] % 256

= [116 + "a"] % 256 → decimal dari "a" = 97

= [116 + 97] % 256

= 213 % 256

J = 213//

Swap [S[i]], S[J]]

Swap [S[1]], S[213]]

Array S = [45, ~~1~~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 → decimal 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, ~~1~~116, . . ., 210, 211, 212, $\overset{1}{\cancel{213}}$, 214, . . ., 250, 251, 252, . . .,
253, 254, 255].

* Iterasi keempat i = 3

J = 71

J = [J + S[i] + k[i % len [k]] % 256

= [~~..~~ 71 + [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, . . ., 109, 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 % len[k]] % 256

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

= [191 + 4 + k[4]] % 256

= [195 + "t"] % 256 → desimal "t" = 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, 25

* iterasi keenam → i=5

J = 55

J = [J + S[i] + k[i % len[k]]% 256

= [55 + S[5] + k[5%8]] % 256

= [55 + 5 + k[5]] % 256

~~= [60 + [illegible]]~~

= [60 + "w"] % 256 → desimal "w" = 119

= [60 + 119] % 256

= 179 % 256

J = 179

Swap [S[i], S[J]]

Swap [S[5], S[179]]

Array S = [115, 213, 71, 191, 55, 179, 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 = 179

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

= ~~[179 + 6 + k [6]]] % 256~~

= [179 + s[6] + k [6% 8]] % 256

= [179 + 6 + k ~~[6%8]~~ [6]] % 256

= [~~8~~180 + "a"] % 256 → desimal "a" = 97

= [180 + 97] % 256

= ~~277~~ 277 % 256

j = 21

swap [s[i], s[j]]

swap [s[6], s[179]]

Array s = [115, 213, 71, 191, 55, 179, 21, 7, 8, ..., 19, 20, 6, 22, 23, ..., 53, 59, 9, 56, 57, ..., 69, 70, 2, 72, 73, ..., 113, 119, 0, 116, 117, ..., 172, 173, 5, 175, 176, ..., 189, 190, 3, 192, 193, ..., 211, 212, 1, 219, 215, ..., 250, 251, 252, 253, 259, 255].

* iterasi kedelapan → i = 7

j = 21

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

= [21 + s[7] + k[7 % 8]] % 256

= [21 + 7 + k [7]] % 256

= [28 + "1"] % 256 → desimal "1" = 49

= [28 + 49] % 256

= 77 % 256

= 77

swap [s[i], s[j]]

swap [s[7], s[77]]

Array s = [115, 213, 71, 191, 55, 21, 77, 8, ..., 19, 20, 6, 22, 23, ..., 53, 69, 9, 56, 57, ..., 69, 70, 2, 72, 73, 79, 75, 76, 7, 78, ..., 113, 119, 0, 116, 117, ..., 172, 173, 5, 175, 176, ..., 189, 190, 3, 192, 193, ..., 211, 212, 1, 219, 215, ..., 250, 251, 252, 253, 254, 255].

* Algoritma : Pseudo-random Generation Algoritma

Array S = [115, 213, 71, 191, 55, 179, 21, 77, 8, ..., 19, 20, 6, 22, 23, ...,
53, 54, 9, 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, 1 214, 215, ..., 250, 251, 252, 253, 254, 255]

Plaintext = "20081"

* 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, 149, 21, 77, 8, ..., 19, 20, 6, 22, 23, ...,
53, 54, 1, 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
t = [S[1] + S[213]] % 256
= [1 + 213] % 256
= 214.

→ u = S[t]

= S[214] = 214 → = 11010110

→ C = u ⊕ P [idx]

= u ⊕ P [0]

= u ⊕ "2" ⟶ biner "2" = 110010

= 11010110

0011 0010 ⊕

C = "ä" didefinisikan 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

= ~~20~~ 284 % 256

= 28

swap[S[i], S[J]]

swap[S[2], S[28]]

~~Ar~~ Array S = [115, 1, 28, 191, 55, 179, 21, 77, 8, ..., 19, 20, 6, 22, 23, ...,
26, 27, 71, 29, 30, ..., 53, 54, 9, 56, 57, ..., 69, 70, 2,
73, 74, 75, 76, 7, 78, ..., 113, 114, 0, 116, 117, ..., 172,
173, 5, 175, 176, ..., 189, 190, 3, 192, 193, ..., 212, 213,
214, 215, ..., 250, 251, 252, 253, 254, 255].

→ t = [S[i] + S[J]] % 256

= [S[2] + S[28]] % 256

= [28 + 71] % 256

= 99 ~~95~~ % 256

= 99

→ u = S[t]

= S[99]

= 99 → biner 99 = 1100011

⟶ C = u ⊕ P[idx]

= u ⊕ P[1]

= ~~0~~u ⊕ "0" → ~~binek~~ biner "0" = 110000

= 1100011

110000 ⊕

1010011

C = "S", desimal = 83

* Iterasi ketiga → Idx = 2

i = 2 , j = 28

→ i = [i+1] % 256
= [2+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]]

Array S = [115 , 1 , 28 , 219 , 179 , 21 , 77 , 8 , ... , 16 , 17 , 55 , 19 , 20 , 6 , 22 , 23 , 24 ,
25 , 27 , 71 , 29 , 30 , ... , 53 , 59 , 9 , 56 , 57 , 69 , 70 , 2 , 73 , 74 ,
75 , 76 , 7 , 78 , 79 , ... , 113 , 119 , 0 , 116 , 117 , ... , 172 , 173 , 5 , 175
176 , ... , 189 , 190 , 3 , 192 , 193 , ... , 212 , 213 , 219 , 215 , 216 , 217 ,
218 , 191 , 220 , ... , 253 , 254 , 255].

→ t = ~~S[i]~~ [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 ⊕ "8" → biner "8" = 111000
= 10011010
  00111000 ⊕
  11100111

c = "G" , desimal = ~~[illegible]~~ 231

* iterasi: keempat → 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

= 279 % 256

= 18

Swap[S[i], S[j]]

Swap[S[4], S[18]]

Array S = [115, 1, 28, 219, 18, 179, 21, 77, 8, ..., 16, 17, 55, 19, 20, 6, 72,
23, 24, 25, 26, 27, 71, 29, 30, ..., 53, 54, 1, 57, 69, 70, 2, 73,
74, 75, 76, 7, 78, 79, ..., 113, 114, 0, 116, 117, ..., 172, ...,
173, 5, 176, ..., 189, 190, 3, 192, 193, ..., 212, 213, 214,
215, 216, 217, 218, 191, 220, ..., 253, 254, 255].

→ t = [S[i] + [j]] % 256

= [S[4] + S[18]] % 256

= [18 + 55] % 256

= 73

→ v = S[t]

= S[73]

= 73 → biner 73 = 1001001

→ C = v $\oplus$ P[idx]

= v $\oplus$ P[3]

= v $\oplus$ "1" → biner "1" = 110001

= 1001001

110001 $\oplus$

1111110

C = "b", desimal = 254 //