No.
Data :

Nama : Ita Puspita .S
Nim : E1E1 20 072
Mk : kriptografi

Tugas

* Algoritma : key - scheduling Algoritma (KSA)

kunci = "Saputra1" , len (k) = 8

Array S = [0, 1, 2, 3, 4, 5, 6, 7, 8, ..., 100, 101, 102, 103, ...
253, 256, 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, 255]

* Iterasi kedua → i = 1
j = 115
⇒ j = (j + s[i] + k[i % len(k)]) % 256
= (115 + s[1] + k[1 % 8]) % 256
= (115 + 1 + k[1]) % 256
= (116 + "a") % 256 ⇒ desimal dari "a" = 97
= (116 + 97) % 256
= 213 % 256
j = 213

swap (s[i], s[j])
swap (s[1], 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]

No.
Date

* 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

= 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,
..., 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 + "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, 243, 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 % len(k)]) % 256

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

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

= (195 + "t") % 256 ⇒ desimal dari "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, 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 ke enam → i = 5

j = 55

~~⇒ j = (j + s[i] + k[i]~~

Iterasi ke enam → 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 + "r") % 256 ⇒ desimal "r" = 114

= (60 + 114) % 256

= 174 % 256

j = 174

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

Swap (s[5], s[55])

Array s = [115, 213, 71, 191, 55, 174, 6, 7, 8, ---, 53, 54, 9, 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 % 8]) % 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

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

= (28 + "1") % 256 → desimal "1" = 49

= (28 + 49) % 256

= 77 % 256

j = 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, 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]

* Algoritma : Pscudo-random generation Algoritham (PRGA)

Array S = [115, 213, 71, 191, 55, 179, 21, 77, 8, ..., 19, 20,
6, 22, 23, ..., 53, 54, 9, 56, 59, ..., 69, 70,
2, 72, 93, 79, 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]

Plaitext : " 2072 "

* 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, 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, ..., 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" = 00110010
= 11010110
00110010 ⊕
11100100

c = "ä", 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, 179, 21, 77, 8, ..., 19, 20, 6, 22, 23, ..., 26, 27, 71, 29, 30, ..., 53, 54, 4, 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 % 256

= 99

$\Rightarrow u = s[t]$

$= s[99]$

$= 99 \rightarrow$ biner $99 = 1100011$

$\Rightarrow C = u \oplus p[idx]$

$= u \oplus p[1]$

$= u \oplus$ "0" $\Rightarrow$ biner "0" $= 110000$

$= 1100011$

$110000 \oplus$

1010011

C = "s", desimal = 83

* Herasi ke Tiga → idx = 2

i = 2
j = 28

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

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

~~swap (s[i]) % 256~~
~~swap (s[3], s~~

swap (s[i], s[j]) % 256
swap (s[3], s[219]) % 256

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

No
Date

=> u = S [t]
= S [154]
= 154 => biner 154 = 10011010

=> c = u ⊕ p [idx]
= u ⊕ p [2]
= u ⊕ "7" => biner "7" = 00110111

= 10011010
00110111 ⊕
10101101

Desimal = 173 ascii : (kosong)

Iterasi ke 4 → idx = 3

i = 3
j = 219

⇒ i = (j + 1) % 256
= (3 + 1) % 256
= 4

⇒ j = (j + s[i]) % 256
= (219 + 55) % 256
= 274 % 256
j = 18

swap (s[i], s[j]) % 256
swap (s[4], s[18]) % 256

⇒ t = (s[i] + s[j]) % 256
= (s[4] + s[18]) % 256
= (18 + 55) % 256
= 73 % 256
= 73

⇒ u = s[t]
= s[73]
= 73 ⇒ biner 73 = 01001001

No
Date

$C = U \oplus P[idx]$

$= U \oplus P[9]$

$= U \oplus$ "2" $\Rightarrow$ biner "2" = 00110010

$= 01001001$

00110010 $\oplus$

01111011

dec : 123

ascii : {