```
NIM
        FIEI 20 090
· Algoritma: key · Scheduling Algorithm (KSA)
  kunci: "Saputral", len (u) = 8
  Array S: [0,1,2,3,4,5,6,7,8..... 100, 101, 102, 103, ...., 253, 254, 255]
 · Iterasi pertama -> 1 = 0
   2-0
   => j = (j + S[i] + K[i mod len(L1]) mod 256
       = (0+0 + k(0 %8)) % 256
       = (K(01)% 256
       = ("s") % 256 => nilai desimal dari "s" - 115
       2 115 % 256
    j = 115
   Swap (s[:]), s[j])
   Swap (S[0], S[115])
Array 5 = [115, 1, 2, 3, 4, 5, 6, 7, ..., 110, 111, 112, 113, 114, 0, 116, 117, ...., 250, 251, 252,
          233,254,255]
  · Iterasi kedua -> i=1
    7 = 1/2
   ⇒ j= (j+5[i] + u[i % len(u)]) % 256
        = (115 + 5[i] + k[i% 8])% 256
       = (IU+ 1+ K[1]) % 256
        = (116 + "a") % 256 => desimal dari 'a" = 97
        = (116 + 97)% 256
       - 213 % 256
    j = 213
   Swap (S[i], S[i])
  Surap (5[i], 5[213])
 Array S=[115, 213, 2, 3, 4, 5, 6, 7, ..., 12, 113, 114, 0, 116, ..., 210, 211, 212, 1, 214, ...
           250, 251, 252, 253, 254, 285]
· Iterasi ketiga -> i=2
  J = 213
  => j = (j + 5[i] + k[i% len(u)]) % 256
      = (213+5[7]+4[7 % 81) % 256
      = (213 + 2+ KB]) % 256
      = (215+ "p") 8/0256 => desimal dari "p" = 1/2
      = (215+112) % 256
      = 327 % 256
51DU % 256
```

1

Nama: Raihan De Laindi

```
J=71
Swap (5[i], 5[i])
  Swap (5 (2], 5 [71])
Array 5 = [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 keempar -> 1=3
   J = 71
  => j=(j + s[i] tu[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
    = \91 % 256
  J = 191
  Sugp (S[i], S[j])
  Swap (5[3], 5[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,...,250,251,252,253,254,285]
· Iteras: kelima -> i = 4
   J=191
  j = (j+ s[i]+ k[i% len (u)]) % 256
    = (191+ S[4] tu[4 % 8])% 256
    = (191+ 4+ k[4]) % 256
    = (195+ "4") % 256 => desimal dari "u"=118
    · (195 +116) % 256
    = 311 % 256
  J = 55
 Sugp (5[i], 5[j])
 Swap (5[4], 5[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 → 1 = 5
   J = 55
  => j = (j + 5 [i] + k [i % len (u)]) % 256
      = (55+5[5]+ L[5% 8]) % 256
      = (60 + "r") % 256 => desimal dari "r" = 119
      = (60+114)% 256
      - 174 % 256
      = 174
Array 5 = [115,218, 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)
   · Iteras: ketývh -> i=6
   J = 174
   ] = ()+5[i]+ [i % len(u)]) 1/0 256
      = (174+5[6] + 4 [6 % len (4)]) %= 256
      = (179+6+ K[6]) % 256
      = (180 + "a") % 256 desimal dari "a" = 97
      3 (180 + 97) % 256
     = 277 % 256
   J = 21
 Swap (5[:], 5 [:])
 Swap (S [6], 5 [174])
Array 5 - [115, 213, 71, 191, 55, 174, 21, 7, 8, .... , 19, 20, 6, 22, 23, ...., 53, 54, 4,
         56, 56, .... , 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
         254,2551
 · Iterasi ke delapan -> i=7
  3 = 21
  j = (j + 5 [i] + k[i% len(k)])% 286
   · (21 + 5 [7] + L [7 % &]) % 256
  = (28+"T") 0/0 256 destinal dari "[" = 49
   ~ (28 + 49) % 256
   = 77 % 286
 J = 77
Swap (S [i], S [j])
Swap (5[7], 5[7])
```

Array s	=[115,213,74,191,55,21,77,8,,19,20,6,22,,53,54,4,56, 69,70,2,72,73-;74,75,76,74,78,,113,114,0,116,117,,172,173,5, 175,,189;190,3,192,193,,211,212,1,214,215,250,251,252 253,259,255]
	A.
16	The state of the s

11109 5 :1116 213 71 . [9] 66 174 21 77 8 .	,19,20,6,22,23,,53,54,4,56,56,
	, 113, 114, 0, 116, 117,, 172, 173, 5, 175, 176,
	, 214, 215,, 250, 251, 252, 253, 254, 25
Plainteus : "2090"	
Iterasi pertama -> ldx . 0	
i = 0	
j = 0	
=> i = (i+1) % 256	274 P. 2872, 28 A. P. 1256
= (0+1) % 256	TENTE STORY
= 1 % 256	(77.12.515) rang
•_(1	Call Class
=> j = (j + s[i])% 256	THE STATE OF STATE OF STATE
	Carrent at A ta at a
= (0+ 213) % 256	12 75/ 1 20/ 51, 44, 51/
= 213	ri ga da na ma
Swap (S [i], S [j])	TRUTT * MIDDLE
Swap (S[1], S[213])	52 0 103 2 103 2 10 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1
1 / 2=131 21	
	20, 6, 22, 23, 53, 54, 4, 56, 57,
Array 5:[115,1,71,191,55,179,21,77,8,,19,69,70,2,72,73,74,75,76,7,78,,11	3,114,0,116,117, 172, 178, 5, 175, 176,
Array S=[115, 1, 71, 191, 55, 174, 21, 77, 8,, 19, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78,, 11 189, 190, 3, 192, 193,, 212, 213, 214,	3,114,0,116,117, 172, 178, 5, 175, 176,
Array 5 = [115, 1, 71, 191, 55, 174, 21, 77, 8,, 19,	3,114,0,116,117, 172, 178, 5, 175, 176,
Array S=[115, 1, 71, 191, 55, 174, 21, 77, 8,, 19, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78,, 11 189, 190, 3, 192, 193,, 212, 213, 214,	3,114,0,116,117, 172, 178, 5, 175, 176,
Array S=[115, 1, 71, 191, 55, 174, 21, 77, 8,, 19, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78,, 11 189, 190, 3, 192, 193,, 212, 213, 214, => f = (5(i) + 5[j]) % 256	3,114,0,116,117,,172,175,5,175,176, .,250,251,252,253,254 [255]
Array S: [115, 1, 71, 191, 55, 174, 21, 77, 8,, 19, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78,, 11 189, 190, 3, 192, 193,, 212, 213, 214, => f = (5(i) + 5(j)) % 256 = (5(1) + 5(213)) % 256	3,114,0,116,117, 172, 175, 5, 175, 176,
Array $S = [115, 1, 71, 191, 55, 174, 21, 77, 8,, 19, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78,, 11 [89, 190, 3, 192, 193,, 212, 213, 214,] P = (S(i) + S(j)) \% 256 P = (S(i) + S(213)) \% 256 P = (1 + 213) \% 256$	3,114,0,116,117,,172,175,5,175,176,
Array S: [115, 1, 71, 191, 55, 174, 21, 77, 8,, 19, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78,, 11 [89, 190, 3, 192, 193,, 212, 213, 214,] => f = (S[i] + S[j]) % 256 =(S[i] + S[213]) % 256 =(1 + 213) % 256 =214	3,114,0,116,117,,172,175,5,175,176,,250,251,252,253,254 [255]
Array $S = [115, 1, 71, 191, 55, 174, 21, 77, 8, \dots, 19, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, \dots, 11 $	3,114,0,116,117,,172,175,5,175,176,,250,251,252,253,254 [255]
Array $S = [115, 1, 71, 191, 55, 174, 21, 77, 8, \dots, 19, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, \dots, 19, 189, 190, 3, 192, 193, \dots, 212, 213, 214, \dots => \forall = (\forall [i] + \forall [j]) \% 256 = (\forall [i] + \forall [213]) \% 256 = (1 + 213) \% 256 = 214 => \alpha = \forall [1] = \forall [214] = 214 => \forall \text{ biner } 214 = 11010110 => \cap = \alpha \text{ \text{ \text{biner } } 214 = 11010110} => \cap = \alpha \text{ \text{ \text{biner } } 214 = 11010110} => \cap = \alpha \text{ \text{ \text{biner } } 214 = 11010110}$	3, 114, 0, 116, 117, 172, 175, 5, 175, 176, , 250, 251, 252, 253, 254 [255]
Array $S = [115, 1, 71, 191, 55, 174, 21, 77, 8, \dots, 19, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, \dots, 11, 189, 190, 3, 192, 193, \dots, 212, 213, 214, \dots => \forall = (\forall [i] + \forall [j]) \% 256 = (\forall [i] + \forall [213]) \% 256 = (1 + 213) \% 256 = 214 => \forall = \forall [1] = \forall [214] = 214 \Rightarrow biner 214 = 11010110 => \forall = \forall \Partial \Partial \Rightarrow biner 214 = 11010110 => \forall = \forall \Partial \Partial \Rightarrow biner 214 = 11010110 => \forall = \forall \Partial \Partial \Rightarrow biner 214 = 11010110$	3, 114, 0, 116, 117, 172, 175, 5, 175, 176,, 250, 251, 252, 253, 254 [255]
Array $S = [115, 1, 71, 191, 55, 174, 21, 77, 8, \dots, 19, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, \dots, 11 [89, 190, 3, 192, 193, \dots, 212, 213, 214, \dots] = 7 + = (S(i) + S(j)) \% 256 = (S(i) + S(213)) \% 256 = (1 + 213) \% 256 = (1 + 213) \% 256 = 214 = 34 = S[11] = S[214] = 214 \Rightarrow biner 214 = 11010110 \Rightarrow C = 4 \oplus P[4x] = 4 \oplus P[0] = 4 \oplus P[0] = 4 \oplus P[0] = (101010)$	3, 114, 0, 116, 117, 172, 175, 5, 175, 176, , 250, 251, 252, 253, 254 [255]
Array $S = [115, 1, 71, 191, 55, 174, 21, 77, 8, \dots, 19, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, \dots, 19, 189, 190, 3, 192, 193, \dots, 212, 213, 214, \dots$ $\Rightarrow f = (S[i] + S[j]) \% 256$ $= (S[i] + S[213]) \% 256$ $= (1 + 213) \% 256$ $= (1 + 213) \% 256$ $= 214$ $\Rightarrow u = S[t]$ $= S[214] = 214 \Rightarrow biner 214 = 11010110$ $\Rightarrow C = u \Rightarrow P[Ux]$ $= u \Rightarrow P[O]$ $= u \Rightarrow P[O]$ $= u \Rightarrow u \Rightarrow biner u = u \Rightarrow u \Rightarrow biner u = u \Rightarrow u \Rightarrow$	3,114,0,116,117,2,172,175,5,175,176,
Array $\leq : [115, 1, 71, 191, 55, 174, 21, 77, 8, \dots, 19, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, \dots, 19, 189, 190, 3, 192, 193,, 212, 213, 214, \Rightarrow f = (5[i] + 5[j])\% 256 = (5[i] + 5[213])\% 256 = (1 + 213)\% 256 = (1 + 213)\% 256 = 214 \Rightarrow u : 5[t] = 5[214] = 214 \Rightarrow biner 214 = 1101010 \Rightarrow c = u \oplus P[ux] = u \oplus P[0] = u \oplus P[0] = u \oplus P[0] = 1100100 00110010$	3,114,0,116,117,2,172,173,5,175,176,
Array $S = [115, 1, 71, 191, 55, 174, 21, 77, 8, \dots, 19, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, \dots, 19, 189, 190, 3, 192, 193, \dots, 212, 213, 214, \dots$ $\Rightarrow f = (S[i] + S[j]) \% 256$ $= (S[i] + S[213]) \% 256$ $= (1 + 213) \% 256$ $= (1 + 213) \% 256$ $= 214$ $\Rightarrow u = S[t]$ $= S[214] = 214 \Rightarrow biner 214 = 11010110$ $\Rightarrow C = u \Rightarrow P[Ux]$ $= u \Rightarrow P[O]$ $= u \Rightarrow P[O]$ $= u \Rightarrow u \Rightarrow biner u = u \Rightarrow u \Rightarrow biner u = u \Rightarrow u \Rightarrow$	3,114,0,116,117,,172,173,5,175,176,

```
· Iterasi Keswa -> 1dx - 1
       1= 1
       ) = 213
   => 1 = (1+1) % 256
        - (1+1) % 256
        : 2
  25 1 (11)2 + C): 1 F
       (213.+5[2]) % 256
       · (215 + 71) 1/0 256
       = 284 % 256
       = 28
Swap (5[i], 5[j])
Swap (5[2], 5[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, 1/4, 0, 1/6,
         117, ..., 172, 173, 5, 175, 176, 7..., 189, 190, 3, 192, 193, ..., 212, 213, 219, 213
         ,.., 250, 251, 252, 253, 254, 255]
    => + = (5[i] + 5[i])% 256
         = (5 [2] + 5 [28]) % 256
         = (28 +71)% 256
         = 99 % 256
         = 99
   => u = 5 [+]
         = 5 [99]
         · 99 => biner 99 = 1100011
   >C = U @ P (1dx)
         = U & P [1]
         * u 0 "0" => biner "0" = 110000
         = 1100011
          110000
         1000011
      C = "5" desiman = 83
```

• Herasi ketiga \rightarrow 3×2 1 = 2 , j = 28 \Rightarrow (= (1+1)% 256 = (2+1)% 256 = 3 Swap (5[3]), S[3]) Array $5 = [115, 1, 28, 219, 55, 174, 21.77, 8, 19, 20, 6, 22, 23, 26, 27, 71, 25, 53, 54, 4, 56, 57,, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, 79,, 113, 11 16, 117,, 172, 173, 5, 175, 176,, 189, 190, 3, 192, 193,, 212, 214, 215, 216, 217, 218, 191, 220,, 253, 254, 255] \Rightarrow $	14.0,
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	14.0,
$ \begin{array}{c} \Rightarrow (=(1+1)\% \ 256 \\ = (2+1)\% \ 256 \\ = 3 \\ \\ \text{Swap} \ (S[3]), S[3]) \\ \text{Swap} \ (S[3]), S[219]) \\ \text{Array} \ S = [115, 1, 28, 219, SS, 174, 21, 77, 8,, 19, 20, 6, 22, 23,, 26, 27, 71, 25, 24, 4, 56, 57,, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, 79,, 113, 113, 114, 117,, 172, 173, S, 175, 176,, 189, 190, 3, 192, 193,, 212, 214, 215, 216, 217, 218, 191, 220,, 253, 254, 255] \\ \Rightarrow + *(S[i]) + (S[j]) \% \ 256 \\ = (S[3] + S[219]) \% \ 256 \\ = (219 + 191) \% \ 256 \\ = 2410 \% \ 256 \\ = 3154 \\ \end{array} $	14.0,
" $(2+1)\%$ 256 " 3 Swap $(5[3]), 5[3])$ Swap $(5[3]), 5[219])$ Array $5 = [115, 1, 28, 219, 55, 174, 21, 77, 8,, 19, 20, 6, 22, 23, 26, 27, 71, 25, 24, 4, 56, 57,, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, 79,, 113, 11, 11, 11, 11, 11, 11, 11, 11, 1$	14.0,
Swap ($S[i]$), $S[i]$) Swap ($S[i]$), $S[2i9]$) Array $S = [115, 1, 28, 219, 55, 174, 21, 77, 8,, 19, 20, 6, 22, 23,, 26, 27, 71, 25, 24, 4, 56, 57,, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, 79,, 113, 113, 114, 117,, 172, 173, S, 175, 176,, 189, 190, S, 192, 193,, 212, 214, 215, 216, 217, 218, 191, 220,, 253, 254, 255] \Rightarrow f : (S[i]) + (S[j]) ?0 = 256 = (S[i] + S[i]) ?0 = 256 = (219 + 191) ?0 = 256 = (219 + 191) ?0 = 256 = 410 ?0 = 256$	14.0,
Swap $(5[i])$, $5[i]$) Swap $(5[3])$, $5[219]$) Array $5 = [115, 1, 28, 219, 55, 174, 21.77.8, 19, 20, 6, 22, 23, 26, 27, 71, 25, 26, 27, 29, 29, 29, 29, 29, 29, 29, 29, 29, 29$	14.0,
Swap $(5[3])$, $S[219]$) Array $S = [115, 1, 28, 219, 55, 174, 21, 77, 8, \cdots, 19, 20, 6, 22, 23, \cdots, 26, 27, 71, 25, 53, 54, 4, 56, 57, \cdots, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, 79, \cdots, 113, 116, 117, \dots, 172, 173, 5, 175, 176, \dots, 189, 190, 3, 192, 193, \dots, 212, 214, 215, 216, 217, 218, 191, 220, \dots, 253, 254, 255] \Rightarrow + \cdot (5[i]) + (5[j]) \% 256 = (5[3] + 5[219]) \% 256 = (219 + 191) \% 256 = 410 \% 256$	14.0,
Array $S = [115, 1, 28, 219, 55, 174, 21, 77, 8, \dots, 19, 20, 6, 22, 23, \dots, 26, 27, 71, 25, 53, 54, 4, 56, 57, \dots, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, 79, \dots, 113, 113, 116, 117, \dots, 172, 173, 5, 175, 176, \dots, 189, 190, 3, 192, 193, \dots, 212, 214, 215, 216, 217, 218, 191, 220, \dots, 253, 254, 255] \Rightarrow f = (S[i]) + (S[j]) \% 256 = (S[i] + S[219]) \% 256 = (219 + 191) \% 256 = 410 \% 256 = 154$	14.0,
$53, 54, 4, 56, 57, \dots, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, 79, \dots, 113, 116, 117, \dots, 172, 173, 5, 175, 176, \dots, 189, 190, 3, 192, 193, \dots, 212, 214, 215, 216, 217, 218, 191, 220, \dots, 253, 254, 255] \Rightarrow + : (5[i]) + (5[j]) \% 256 = (5[i]) + (5[i]) \% 256 = (219 + 191) \% 256 = 410 \% 256$	14.0,
$116,117,,172,173,5,175,176,,189,190,3,192,193,,212$ $214,215,216,217,218,191,220,,253,254,255$ $\Rightarrow + * (5[i]) + (5[j]) % 256$ $* (5[3] + 5[219]) % 256$ $* (219 + 191) % 256$ $* (410 % 256)$	213,
21 4, 215, 216, 217, 218, 191, 220,, 253, 254, 255]	103 103 104
=> + = (5[i]) + (5[j]) % 256 = (5[3] + 5[219]) % 256 = (219 + 191) % 256 = 410 % 256 = 154	100 P
2 (5[3] + 5[219])% 256 2 (219 + 191)% 256 2 (10 % 256 2 \54	STA
2 410 % 286 2 154	
2 \54	
2 154	
2) u = S[+]	-
= 5[154]	
- 154 biner 154 = 10011010	
⇒ C 2 U ⊕ P [18x]	
= u e p [2]	
= u & "g" => biner "g" = 111 001	
2 100 11010	· ·
1010011	
C: "E"decimal 163	-
1.01/17	
I = I = I + I + I + I + I + I + I + I +	
	-

```
· Iterasi ke empat => ldx = 3
    i=3, j=219
  => 12 (1+1) % 256
     = (3 + 1) 1/0 256
  254 ([i]2+ (j+ S[i]) %256
      = (219+5[4]) % 256
   = (2191 55)% 256
     = 274 % 256
8/1= 115
Swap (S[:], S[:])
Swap (5[4], 5[18])
Array S = [115, 1,28,29, 18, 174, 21, 77, 8, ..., 16, 17, 55, 19, 20, 6,22, 23, 24, 25, 26
         27,71,29,36, ...,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, 2, 192, 193, ..., 212,
        213, 214, 215, 216, 217, 218, 191, 220, ..., 253, 254, 255]
    >+= (S[i]+ S[)]% 256
       = (5[4] + 5[18] % 256
       = 18 + 55 % 256
       2 73
   => u = S[+]
       - 5 [73]
       = 73 => biner 73 = 1001001
  => C = U @ P [ Idx]
       2 4 0 P [3]
       = U 0 "0" => biner "0": 110000
       100/001
           110000
          1111001
    C = "y" desimal = 121
```