	No.
	Date:
Nama : Ilmi Faizan	
NIM : EIEI20011	
	James - Jak Korn (darder 300) 2 / Larger S
	200 8000 912 \$ 1 miles
* Algoritmo Key Scheduling Agorithm (KSA)	AR 'A L'OUR STATE
Array S = [0,1,2,3,4,5,6,,253,254,256]	Committee of the 10 and 10 mines. I see so
Kunci = Saputral -> Panjary = 8 karakte	
1) $i = 0, j = 0$	SWap (S[i], S[j])
j = (j + s[i] + k[i mod length(kunci)])	
j = (0+0+ k[0)) mod 256	1
j = 115 mod 256	and the second of the second o
j = 115	1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -
Array S = (116, 1,2,3,4,, 114,0,116,)	, 253, 254, 255
The second secon	(0) 3 (0) - (0) 2 (0) (2 (0) 4 (0) 3
2) i = 1. j = 115	
	Swap (S[i], S[j]) += = = = = = = = = = = = = = = = = = =
$j = (16 + 97) \mod 256$	1 Sulap (1.213)
j = 213 mod 256	3) 20027 305 popul (ES + 081) = 1
j = 213	Complete and the Country of State Control of the Country of the Co
Array 5 = [115, 213, 2, 3, 4,, 114, 0, 116,.	, 212.1, 219, 253. 254. 256]
25.6 22, 360 476 3 102 92 - M C 18 -	1909 S = [19, 28, 71, 191 05, 210 21, 7, 8,
3) (=2, j=213	118 2018.001 3611.6.851
$j = (213 + 2 + k[2]) \mod 256$	Surap (SCi), SCj)
$j = (215 + 112) \mod 256$	swap (2, 71)
j = 327 Mod 256	(= (1+++k(1)) med secon (++)
j = 71	41 2 (20 + 37) = 1
Arroy S = [115, 213, 71, 3,4,, 70,2,9	2 114, 0, 116,, 212, 1, 214, 253, 254, 255
	77 62 7 6.02 1 38 TAR F 1 7 F 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	P. S. F. L. D. DY THE PRINCIPLE STORY BERTH.
j= (71+3+ k[3)) mod 256	
j= (74 + 117) mod 256	Suop (3, 191)
j = 191 Mod 256	
J= 191	
	12.72, 114,0.116,, 190,3, 192,, 212.1. 214
253, 254, 255].	

	Date:
5) i=4, j=191	Califor Hill of State ompiles
j=(191+4+k[4]) mod 276 Swap (S[i), S[i])	Marie de Baron
j= (195 + 116) mod 256 swap (4, 55)	Something of the state of the s
j = 311 mod 25C	
j = 55 (cgs) saltage	A . waster toy sales . A
Array S = [115.213,71.191,55,5,6,, 59.4,56,, 70.2,72,	,119.0.116, 190.3.192, 212,11
214,, 253,254,255],	Man = Sentral + Decide
The state of the s	
6) (= 6, j = 65 (/z) 10 0?	0=1-0=1111
j= (55 + 5 + k(5)) mod 256 swap (S[i], S[j])	1= (1+ 5/1) + kg mou
j = (60 + 114) mod 256 swap (5. 174)	« (Cald + %0 + 0) = 1
j = 174 mod 296	Dec Link all = i
j = 174	-au = 1
Atray S = [116,213,71,191,56,174,6,7,, 54,4,56,,70,2,72	114,0116, 173,5,175
190,3,192, 212,1,214,, 253.259.255).	
	au a f c. l'an f (c.
	(bon] 4 + + an / 5 + 1
j = (174 + 6 + k(6)) mod 276 Swap (SCiJ, SCiJ)	
j= (180 + 97) mod 296 swap (6, 21)	20Mil 210 210 210 210 210 210 210 210 210 210
$j \approx 277 \mod 296$	E 213
j = 21 532 rec 882 123 held 240 ml	And the second s
Array S = [115, 231.71.191.05,174,21,7,8,, 20,6,22,, 54	9,4.56,, 70,2,72,, 119,0,116,
173,5,175 190,3,192 212,1,249,, 253,2	254.265]
- 1 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2	mc([0]4 + 2 + 212)= join
	1900 (30 +3 -5.) = 1 -5.
j = (21+7+ k[7]) mod 256	sat pole title =)
j = (28 + 49) mod 256	
J = 77 Mod 256	Edface all a trianal
J = 77	
Arry S = [115, 231, 71,191, 55,174, 21, 77, 8, 9,, 20,6,22,	. 54.4.56 70, 2, 72 76.7.78.
, 114.0, 116,, 173.5, 175, 190,3,192,, 2	212.1.214,, 253, 254, 255]
266 (30 (40 (50 days))	Some (int + hi) all the
	376 900 M = 1
3). 4 8 mg 70 3 3 mm a 4 0 0 1 5 mm 3 4 0 3 19 2 mm 2 9 mm 2 mm	THE COUNTY SECTION

```
* Algoritma Pseudo-randon generation algorithm (PRGA)
   Array S = [115, 213, 71. 191. 55, 174, 21, 77. 8.9, ..., 20, 6, 22, .... 54, 4, 56, ..., 70, 2, 72, 72, ..., 76.7, 78,
                ..., 114,0,16,..., (73,5,175, ..., 190,3, 192, ..., 212,1,214, ..., 253,254,155)
    Plaintext = "201"
   1) idx = 0, i=0, i=0
                                           => 1= (j+s(i)) mod 256
       => i = (i+1) mod 256
                                               = (0+S(1)) mod 256
            = (0+1) mod 256
      Swap (SC1), SC1) & Swap (-213, 1)
      Swap (S(1), S(213)
       Array S = [115, 1.71, 191, 56, 174, 21, 77, 8, ..., 20, 6, 22, ..., 59, 4, 56, ..., 70,2.72, ..., 76, 7,78,
                   ..., 114,0116, ..., 173,6,175, ..., 190,3,192, ..., 212, 213, 219.... 253, 254, 255]
                                            => c = U + PLlax)
       $ t = (SCi) + SCj) mod 256
             = (5(1) + 5(213)) Mod 256
                                                  = u & p[0]
                                                  = U # "2"
                     + 213) mod 256
                                                  = 11010110 = 1
             = 214
                                                     00110010
        ⇒ u = s[t]
                                                     11100100 -> kanversi kederimal
             35 5[214] (3) 2 + 915
              = 214 == WOIOIIO =
                                               C = 228 -> a
    2) (dx = 1, (=1, ) = 213
    \Rightarrow i = (i+1) \mod 256 \Rightarrow j = (j+s[i]) \mod 256
                                               = (213 + 71) mod 256
            = (1ti) mod 256
                                         28
      Swap (SLi), SLj)) P swap (71, 28)
      swap ( S[2], S[28) -
      Array 5 = [115, 1, 28, 191.55, 174, 21, 77, 8, ..., 20, 6, 22, ..., 27, 71,29, ..., 54, 9,56, ...,
                  70,2,72. ..., 76.7,78, ..., 114.0,116, ..., 173.5,176. ..., 190.3,192. ..., 2/2,2/3.
                  214, ..., 263, 254, 255].
                                             => c = u & P[idx]
       = ( S[i] + S[j]) mod 258
            = ( S[2) + S[28)) med 256
                                                   = u & P[I]
                                                   = U + "0"
            = (28 + 71) Mod 256
                                                   = 01100011
            = 99
                                                      000110000
       => u = s(t)
                                                     0.1010011 -> Konnert ke desimal
             = 5[99]
                       = 01100011
                                                 C = 83 \rightarrow 5
             = 99
                                                                                  444
```

```
3) idx = 2, i = 2, j = 28
                                         ⇒ j = (j+s[i]) mod 256
   ⇒ i = (i+1) mod 250
        = (2+1) mod 250
                                             = (28+191) Mod 256
                                            72 219 31.0
    Swap (SCi), SCj)
                            Supp (191, 219)
    swap (S[3), S[219)
    Array 5 = [115,1.28,219,56,174,21.77, 8, ..., 20,6.22,..., 27.71,29,-.., 54,4,56,,...,70.2,72,...
              76.7.78, ..., 114,0.116. ..., 173,5,176, ..., 190,3.192, ..., 212,213,214..... 218,191,220,...
              253,254,255]
   => t = (SCi] + S[i]) mod 256
                                       => c = u + P[idx]
         = (S[3) + S[219]) Mod 256
                                             = U D P[2]
                                             = U 0 "1"
         = (219 + 191) mod 256
         = 154
                                             = 10011010
    => u = 5(t)
                                            00110001
          = 5[154]
                                            10101011 -> konsut te desimal
                                     1
                                           C=171 -> 44
          = 154
                    = 10011010
4) idx = 3, i = 3, j = 219
    => i = (i+1) mod 276
                                         = j = (i + S[i]) mod 256
         = (3+1) mod 266
                                              = (219+5[4]) mod 256
                                              = (219+55)=mod 256 = 18
   Swap (SLi], SLj])
                          57 Swap (55, 18)
   swap ( S[4), S[18])
                                                      2) (dx = 1 1 = 1 10 213
    Array S = [115, 1, 28, 219, 18, 174, 21, 77, 800 , 17, 55, 19, 20, 6, 22, ..., 27, 71, 29, ..., 59.4, 56.
               ..., 70,272,..., 76.3.78, ..., 114,0,116..., 173,5,175,...,196,3,192,..., 212,213,214.
               ..., 218,191,220. 25 253,259,255].
    => E = (S[i) + S[j]) mod 256
                                         >> C) soul OF P[ldx]
          = (S[4] + S[18]) mod 256
                                               = U D P[3]
          = (18 + 55) MOD 256
                                               ~ U ⊕ "1"
          = 73
                                            2 = 301001001
     JU= S[t]
                                             00110001
                                                  01111000 -7 konversi ke desimal
          = S[73] (x6] 19 9 0 =
                                             C = 120 7 X
                    = 0(001001 :
    Plaintext =
                  2011 0 0 0 0 0
    EAKnipsi
                 äSux
```