```
Mama: Febriansyah
MIM
      : F1E1 20 06B
      · Genap
Kelas
  Tugas Kriphografi
                                 200 X ( [ 5] 16 5 60 10)
      Key Scheduling Algorithm (KSA)
K= Saputra1 => Ko=S, K1=9, K2=P, K3=4, K4=+, K5=r, K6=9, K7=)
 Array S = [0,1,2,3,4,5,6, ..., 245,246, 247, 248, 249, 250, 251, 252, 253, 254,255]
  laran' pertama
  200
  . o> j= (i+s (i)+ K [i mod len (k)]) mod 2 FC 1
       = (0+0+k [0%8]) % 256
        = (K[0] %. 256
                                     gal so tay ment mention
        = ("s") / 256 => nilai desimal dari "s" = 115
        - 115 %. 25%
       1 = 115
       swar (scij, scij)
       Swap (2 [0], 5 [115])
    array 1 = [115, 1,2,3, 4,5,6,7, ..., 110, 111, 112, 114, 0,116, 117, ..., 119, 200,
             201, 202, 203, 204, 205, __,250, 251, 257, 253, 254, 255]
   Iterasi kedua - isl
      3=118
      => > j = (1+s(i) + k [i/ len(k)]) /2276
           =(115+5(1)+[128]) 12 256 00 10 213 0 210
      = (115+1+K[1]) % 256
           = (116 + "a") %. 256 => definal dan "a" = 97
            = (116 tg7) 1. 256
            = 213% 256
          j = 213
         Swap = (8Ei), sEij)
         Swap , (S[I], S[213])
          Array 5 = [115, 213,2,3,4,5,6,7, ..., 112, 113, 114,0,116, ...,210,211,
                  212, 1, 214, ..., 250, 251, 252, 253, 254, 255)
           (2) 2 ( 1) 1 1) good
```

```
1thrati ketiga -> 1=2
 j = 213
  -> j= (j+s [i]+k [i% len (k) ]) % 2rl
       = (213 +5 [2] + K[2/8])% 256
        = (213+ 2++[2]) / 25C
       = (215 + "p") 2756 => derimal devi "P"=112
      = (215 + 112) % 256
       = 327 % 256
     Swap (ILI], ILI]
      Ewap ( 5[2], 5[71])
     Array S = [115, 213, 71, 3, 4, 5, 6, 7, -, (9, 70, 2, 72, -, 112, 113, 114, 0, 116, -,
               210, 111, 272, 1214, -, 200, 251, 252, 253, 254, 255]
 Heran Frempat -> 1-3
   J= 71
   -> je (j+s[i]+k [i% ken(k)]) % 266
        = (71 +5537+ K(3281) % 256
         = (31 +3+ K(3)) 1/2 256
                                       (((1)) 1 ((1)) gen?
         = (74+"4") %. 216 => definal dain "U"=177
      2 (34 + 117) % 26 5 100 Has year so s 105
         2 191 % 256
        3 = 191
       Swap = (S[i], S[j])
       Swap = (SE3J, SE1917)
       array 3 = (115, 213, 71, 151, 4,5,6,7, -, bg, 70,2,72,., 112, 113, 114,0,
                116, ..., 189,190, 3,192, -, 40, 21,1,214, -,250, 251,
                252,252, 254, 255 ]
                 1 -4
 Iterati ke lima
   j= 131
    -> j= (j= 5 [i] + Ei % len (K) ]) % 286
        - (191 + 5[4] + F 4 1/8]) / 256
         = (191441647) % 256
         = (1954 "t") 1/206 => defined "t"=116
          = (195+ 116) y. ZFL
                                    Swap (1 [i], 5 [i])
          - 311 % 256
                                    Swap (S[4], S[15))
          2 55
```

Array 5 = [15, 213, A1, 191, 55, 5, 6, 788, ~, 57, 14, 4,56, 17, ~,69, 70, 2,72,73, ~, 113, 114, 0, 116, 117, -, 189, 190, 3, 192, ..., 211, 212, 1, 214, ..., 250, 251, 252, 253, 254, 255) ·) Iterati terram -> 9 =5 1 = 55 => j= (jts Li] + Ei% len (K)]) %256 = (55 +5 ED) + E EC% @ J) %. 286 = (224 24 E [2]) 1/526 = (Got " " ") 1/ 256 =) Doring " +" = 114 - (60+ 114) %256 - (74 % 251 (Add) and read providend makes defend = 17 4 % assa Array 5 = [115, 213, 71, 191, 55, 174, 6,718, _, 13, 54, 4, 56, 57, _ 69,70, 2 72, 73, --, 113, 114, 0, 116, 117, 172, 173, 5, 175, 176, ..., 185, 190, 3, 198 193, .. 211, 212, 21; 214, 215, 2. 250, 251, 252, 253, 254, 255) ·) I teras: to hipsh -> i=6 j = 174 > (1= ()+s ()] + + (i % len (+)) % 1256 len (1) = (174 + 5[6] + E [6 1/0] 1/25 00 00 00 00 00 00 00 00 = (194 + 6+ FCG) % 256 = (180 + "g") 1/286 => derinal a -97 and home fill bill of = [180+ "97)/286 · (277 %. 256 J 2 21 Eworg (S [1] . S [77) (S C67, S [1747) Array S= [115, 213, 71,191,55, 174,21, 7,8, ,, 19,20, 6,22, 13, ... 13. C4, 9,56,57, -, 65, 70,2, 72,7)., 113, 184, 0,16, 117, 192, 173, 5, 175, 176, -1185 190,3:197, 193, -211, 213, 1,214, 215 200, 25 \$1, 252, 253, 254, 255. e) Hercus Kedelapan > 1= 7. 1= 21 = J= (j+s[i]+ k(i % lin(k))) % 786 311 2 (2) +5 \$73 4 \$ (7/2 87) 1/2 756

2 (21+7+ = [7)) % 26

```
= (28 + "1;") 1/2 2063 desinal (" = 49
  2 (20+49) % 256
  2 77 /. 206
          ( 23, SE+7)
   swap (5[7], 5[77)
  Borrey S= [115, 213, 71, 191, 55, 21, 77, 8, -15, 20, 6, 22, 23, -58,14,54, 86, 57, ...) 69, 70, 2, 72, 73, 74, 55, 76, 7, 78-, 113, 114,0,116,
               117, .. 172, 173, 5, 175, 176, -184, 190, 3, 192, 153, -, 211
               2/2, 1, 2/4 1215, -, 250, 251, 252, 253 254, 2550
Pseudo-Random Generation Algorithm (PRGA)
Array 5 = [115, 213,71, 191,55, 174, 21,77, 8,9,10, -, 20,6, 22, -,54, 4,56, ,70,2,72,73, 74,
         35, 76, 7, 78, -, 114, 0,116, -, 183, -, 180, 3, 182, 212, 1, 214, -, 254, 255]
                    THE REST OF THE PERSON
 I terasi pertama
   j = 0
                  P=2047
   100
  for index , 0 to length (p)-1 ( ) and X ( ) a b [ ( ) ]
   For Index = 0 to (4)-1 = 0 to (3)
        i z (oti) mod 256
         12150 A June and
         J = (j+ S[1]) mod 256
         j=(0+213) mod 286
         i = 213
                            S[i]=1 S[j]:213
         SEIZ, SEIJZ
         = S[1], S[213]
                              S [213] + S [1] 2 In Index
                             $ 1 + 213
        t = (s [1] +s [213]) mod 256
 - 1+213 mod 26 = 214
         4 = 5[214]
         C = 40 P [0]
            = 21402
            : 110/0110
              00110010
            11100100
```

teran kedua		50017 2
iel jeus		1077 BV . 5
For index . 0 to (3)		8 8 421 -
i = (i +1) Mod 276		01011001
i = (111) mod 256		a cholida
i= 2		20110101
J= (jts [i]) mod 256		F 651-
j= (213+5[2]) mod 2+6		
j= (213+71) mod 256=284 mo	d 2 rb	francist soull
= 28		elsel fel
		(0) 06 0 : 1 AN 100
(£2) 2 ([£] 2, [1] 2) qow2	287)	de ton (14:7 = 1
t= (5[2] + 5 [28] mod 256		Part of the second of the seco
t: (28+71) mod 216 = 99 1	mod 216	Dark (17 14L) - L
t= 99	450	EN PROTECTION
[ee] 2 = U	1-458-6 36	The Court of the C
(= 4 8 P[i]		\$1 -L
₃ 99 0 0		
		(117 12 (1) x) grand
00110000 = 83=	S (capital s)	
01010011		(8617 1 KEPT 2) = #
	73 000	It have (Start) - down
lterasi ketiga		FF - 1
1=2		7.5%
J = 28		(86)
for index = 0 to 3		93.9 8 80
i = (i+1) mod 256	1001500000	25.
	10010010	
	00011100	1 1
= 3 j = (j+s [i]) mod 256	10001110	
) = (28+5[3]) mod 256	P 8/1=	
j = 219		pr2's' condant
g Swap = (S[i], S[i])		
(S[3], S[210])		· manager that referred
(212), (512)		A second
t= (s [i] +s [219] mod	256	
t = (219+191) mod 256 =1	40 modes6	

No 2 EIRA]	roger zemi
C= Y # P[2]	1.1 jeun
- 154 B6	muka, yohat noh
= 10011010	200 bend (141) of
00110110	275 hear (13+) 21
10101100	5 4
= 172 7	3-, (D124) -L
	and the second of the formation of
I terasi ke empat	and the same of the same of the same
1=3 1=219	82.
for index = 0 to (3)	
i = (i+1) mod 256	(tos), pos?)-(t) + (i)?) pour
i = 4	228 trans [98] 3 4 [63] 1 - 1
	d 256 in stand of another (18+00) of
J= (219 + 1[3]) M	
	od 256 = 274 mod 256 [087 & 419
J= 18	(17 0 0 0)
Supan Citiz	0 \$ 6 8 4
2004 (1[1] 1[1]) = (5[4], s (183) Hapoties
t = (s [4] + s(187)	(8 mm) 2 488 a 20000000
t = (18tos) mod 250	mes 216
t = 73	
77	levoli zelega
4 = 5 [73]	PT - 1
C= 4 @ P [3]	Enlo while of
- 73 ® 8	020 600 (147) - 1
· Openio	01001001 222 (000 (126)
oonioo o	
· Openio	01001001 222 (000 (120) 20
oonioo o	01001001 212 (mm (126) 2.
00 11 000 a	01001001 22 long 8
0011000	01001001 22 long 8 2 long 8 long 8 2 long 8 long
0011000 a 0011000 a 0011000 a Hasilya: 'a's 7 q	01001001 00111000
00 11 000 a	01001001 22 long 8 01110001 22 long 8
0011000 a 0011000 a 0011000 a Hasilya: 'a's 7 q	01001001 22 (mm (1+6) 22 (mm (1
0011000 a 0011000 a 0011000 a Hasilya: 'a's 7 q	01001001 22 (mm (1+6) 22 (mm (1