```
Muhammad Agus Saputra
Mama
MIM
          EIE1 20 039
Kerptografi
                                            ors have [[4 dipro] boys 1] of +
G . [0,1,2,3,4,5,..., 251, 252,253, 254, 255] home [ 8 1000 0]
key = sapulras
KSA
                                                                  12 F Bolto
                                                                            101
    lerast 1
                                               Diende . Isk = , Irla . Isla
          1 = (1 + 5[1] + k[1 mod length (4)]) mod 256
     ( o + o + k[ o mod 8] mod 256
      0 + k[o] | mod 250
       0 + 115
                 mod 256
                      = $[0], $[ns] Dis boin ([d Nigood born /] / + [1]? )!
  swap s[1], s[1]
G = [ 115. 2,3, a,5, ...., 112, 113, 114,0, 116, ...., 258, 254, 255 ] low
    Acrasi 2
 121
1 = 115
J = ( ] + s[i] + k[i mod length k]) mod 256
    (115+ 1 + k[1 mod 8]) mod 256
     [ 116+ k[1] } mod 256
                 mod 255
      116 + 97
      213
  suop s[i], s[1] . 5[i], s[213]
                                                125 Kom [[ 30 Lain #] 4 4
5 = [ 115, 213, 2, 3, 4, ..., 113, 114, 0, 116, ..., 211, 212, 1, 214, ... 253, 254, 255]
 Storasi 3
                                              [MI]E
1 = 2
1 = 213
                                             S = [115, 213, 71, g ..., 70, 2, 71, ... 212,
 3 = (1 + still + klimed length kl) med LEC
                                                   1, 219 , ... , 253 , 259 , 255 ]
  = (213 + 2 f k [2 mod 8]) mod 250
    (215 + k[2]) mod 256
    327 mod 256
  swap s[1], s[7] = s[2], s[71]
```

```
while 2 week tommerche
lerage 4
  1 - 3
 9 2 71
J: (1 + s[i] + k[i mod length k]) mod esc
     = (71+3 + E[3 mod 8]) mod [ 255 , pag , san , sa
             (74 + k[3]) \mod 256
                                               mod 256
              74 + 117
             191 mod 256
                                                                                                                                                                                              1 /runsil
1= 191
      swap s[1], s[7] = s[3], s[191]
   S = [115, 213, 71, 191, 4, ..., 14, 0, 12, ..., 114, 0, 116, ..., 190, 3, 192, ..., 212, 1, 1
                                                                                                        228 Dott [[(2) Hord . 5050 1] 2
               1 .... 1 253 , 254 , 255 ]
                                                                                                                                                       [ 8 60m 0] x 1 0 10
                                                                                                                                                                             1014 4
Herasi 5
  1 = 4
 1 = 191
 9 = (1+5[1] + k[i mod length k]) mod 250 [211] = [211]
                                                                                                                                                                         1112
                                                                                                                                                                                            [1]3
               (195 + F[4]) med 250
                    (195 + 116 | mod 256
                                                                                                                                                                                                               1 = 1
   1 =
                                 55
         swap s[1], s[1] = s[4], s[ss]
                                                                                                                                          [ 4 - Epis Lound 4 + Dile 41
Gerasi C
  1 = 5
                ] + 5[1] + k[1 mod length f] mod 150
                 ( 22 + 2 + k[2 mag 8]) mag 120
                                                                                                                                 Faste File -
                                                                                                                                                                            1012
                          med 256
                          60 + 114 )
  7 2
                               IM
                         s[1], s[1] = s[5], s[1]
                                                                                                                           7 1 = (186 + 97) mod 256
                               1 38 .... $ 1150, 818 , 211 ]
 lerasi 7
                                                                                                                           70 10 DONNE 14 1
  1 = 6
                                                                                                                                     swap s[1], s[1] = s[s], s[21]
  1 = 14
  ) = (1 + 5[1] + k[1 med length k]) med 260
       = ( Aq + 6 + + [ 6 mod 8] mod 256
                                        4[1] mad 256
                                                                                                                                 11112
```

```
Thorast ko o
 1 27
 1 2 W
 ] = (] + s[i] + k[i mod length +] mod 256
   2 (2++2+ +[7 mod 8]) mod 256
      (28 + [7]) mod 256
        (28 + 99) med
 1 2
         77
  swap ([i], sty) = str], ([77]
G = [ 115, 213, 71, 191, 45, 174, 21, 77, 8,9, ...., 19,20,6,20,..., 52,53, 84, 4,4
      ··· , 75 , 76 , 7 , 78 , ... , 113 , 114 , 0 , 116 , ... , 172 , 173 , 5 , 175 , ... , 190 , 3 , 192 , 211 , 212 , 1 ,
      249, ..., 258, 254, 255, 200 ]
 P = 2039
Herast 1
                                        Iterasi 2
                                         1 = 1
1 = 0
                                        1 = 213
J = 0
                                         1 = (+1) mod 250
1 = (0+1) mod 256
                                                      The ball fry
 012 1
 1 2 (] + s[i]) mod 255
                                         1 = (1+ 1[1]) mod 256
                                          2 (213 + 5[2]) mod 416
 = (0+ s[i]) mod ess
                                           = (213 + 71) med 276
 z 0 + 213 mod 256
                                           2 284 med 256
 1 = 213
  swap s[1], s[1] = s[21], s[10]
                                         1 = 28
                                                   The lower
                                         swap s[1], s[1] = s[2], [28]
   1 = 5[1] + 5[1]
                                           1 = 5[1], 5[1]
    t = 1 + 213 = 214
                                             = 71 + 20
  u = 5[24]
    = 219 @ p[0]
                                                  99
                                           u - s[99]
      - 214 6 2
                                              = 99 @ P[e]
     = 11010110
                                                99 (1) 6
          @ 011001100
                                              = 4011 000 11
                      = 228
          11100100
                                                 400110000 G
                                                  01010009 2
```

```
Sterasi 3
 12 2
 1. 28
 1 = (2+1) mod 256
 1= 3
 J= (1+ s[1]) mad 256
    (28 + s[3]) mod 256
    (28 + 191 ) mod esc
                                                     following the same
     219 480
 swap s[1], s[7] = s[3], s[219]
185, 13 . 219, 4, 2191 .... = 2410 2 mod 256 .... 187, 0, por 21, .... 1816, 8, 28 . 28 . 28
  U = ([154]
                                      QW , DV , DV , 824
    = 159 ( p[2]
    2 154 1 3
     01011001 =
       11001100
      10101001 = 169
                                                           1 1200
Sterasi 4.
1 2 3
1 = 219 1/2 hours 1/2 + 17
1 2 (3+1) mod 256
       28.5 0 SW / 1172 + C
  2 9
     (1 + 5[1]) mod 255
1 2
      ( 28 4 5[4]) mod 256
      (28 + 55 ) mod 25C
       83 mod 256
       (832 × 11 Jan 232 gans
      s[1], s[1] = s[A], s[83]
 sway
       s[i] + s[j] + /
       83 + 55
       138
       5 C1387 19 19 18817 2
                                             6 3 0110107/
  U
     2 138 ( ) [3]
       138 (4) 9
       0101010001
       00111001 1
        10110011 = 179
```