```
Nama
        : Deni Hidayat
Nim
        : ELE120026
Makkul : Kriptografi
Soal
1. Veriakan KSA dan encom
                       abangon procented was dan kunci Saputras.
Jawab. 1 1 212, 112, 012, 002, .... , 9, 8, 8, 8, 8, 8, 12, 211) . 2
           S = [0,1,2,3,4,5,6,7,8,9,10,11,...,,56,57,50,...
                250,251,252,253,254,255,256][] 0 + 1, ) +
Dik:
                                  × (213 +2+112) %
                   Longth = 0 -
  K: Saputra1
  ko = 3
            = 115
  k, = a
           =97
  k2 = P
8 = 118, 213, 21, 3, 41, 5, 6,
  Ky = k
  Kr = r
  K6 = a
  k2 = 1
 la J=0 J=0li pertoma
    J = (J+S[i]+ E [i mod length (k)]) mod 256
    J (0) = (0 + 5 (0) + k (0 mod length (8) 7) mod , 256
 12 25 = (0,+0+E (S)) mod 256 191 16 815 217
        = (0+k [115]) mod 256
       = 115 mod 256
   Swap = (SCi], SCJ]) [(1) Adoubl & i) x + [1] 2+ () =
  Swap = (S [0], S [115]) 12 8 (18 3 4) 3 + [+] 2 + [1) 3
      S = [115,1,2,3,4,5,6,7,8,9,10, 3-156,57,50,10,114,0,116,17,...
          253,254,25,256]
```

```
2 200 21313
    * i=1, j=115
      ] = (] + S[i] + E[i % Langth (t)]) % 256
        = (115+ 1 + E[1 % 8]) % 256
        = (115+1+97) % 256
        = 213 % 256
. Electron : 215 m up to the transcript of the transcript of
      Swap (S[1], S[213])
       8 = [115,213, 2,3,4,5,6,7, ..., 209,210,211,212, 1,214, ... 256]
    ] = (] + S(i] + E[i % longth(k)]) % 256
        = (213+S[2]+k(2%8]) % 256
        = (213 +2+112) % 256 7 · dignos
                                        1 codução a M
        = 327 % 256
                                                 6 - 04
        = 71
       Swap ( S[2], S[71])
       5=115,213,71,3,4,5,6,7, ... 69,70,2,72,73, ... 255,256]
    * 1 = 3 , j = 71
      j = (j + S[i] + E[i % Longeli () ]) % 256
        = (71+5[3] + k [3 % 8]) % 256
         =(71+3+117) % 256
         = 191 % 256 smotog (100 depro) bouilde [172+1) = 6
       Swap (S[3] S[191]) 1000 0000 000 4 (0) 21 00 200
       S = [115,213,71,191,4,5,6, ..., 189,190,3,192, ... 255,256]
                          625 poin ([2]] 940
    * 1:4, j:19,
       j = (j+5[1]+K[i % Length (+)]) % 256 133)
         = (191+5[4]+16[4%8]) % 256 3012 (0) 2) = 9000
256 256
         = 311 % 256
         : 55
       swap (S[4], S[SS]
       S = [115, 213, 71, 191, 55, 5, 6, - . , 50, 51, 52, 53, 54, 4, 56, - . , 256]
```

John Pishard

```
kerinkon prof dengan plaintest with den Best Copasie! i *
     j = (j + S[i] + K[i % longth (k)]) % 256
       = (55 + 5[5] + K [5 % 8]) % 256
       = (55+5+114) % 256
                                    Prohibert = 2026
       = 174 % 256
       = 174
                                  - Kunci : Sapution
8 = [115,213,71,191,55,174,6,7,...,173,5,175,176,-.,256]
 * i = 6 , j = 174
    j = (j + S[i] + K[i % longth (k)]) % 256
     = (174 + 5 [6] + 4 [6 % 8]) 6 256
     = (174 + 6 + 97) % 286 1 1 3 + 6)
      = (277) % 256 ([[] 3, []] 3) quod
= 21 82 81 % [[] 2 + [] 2) = }
    swap (S[6], S[21]) (1)2 1)
    S = [115, 213, 71, 191, 85, 174, 21, 7, 8, ..., 20, 6, 22, ..., 255, 256]
 * i = 7 , j = 21
   J = (j + S(i) + K. [i % Longth (k) ]) % 256
      = (21 +5 [7] +1 k [7 % 8]) % 256
     = (21+7+49) % 256
      = 77 % 256
      = 77
     8wap (5[7], 8[77]) ([1]8, [1]8) 9002
     8 = [115, $ 213, 71, 191, 55, 174, 21, 77, 8,9, 9, 73, 74, 75, 76, 7, 78, -
          255,256]
                             2 U @ P(0) = 214 6 2
```

```
2. Kerjakan PRGA dengan plaintext nim dan kunci Saputrati
              9 26 % ([[2]) WELLS !! 1] 21 + [1] 2 + 6) + 6
   Jawab
   - Plaintext = 2026
   - kunci : Saputra1
   -5
          = [115, 213, 71, 191, 55, 174, 21, 77, 8.9, - - 258, 254, 255]
             3 - [ 45, 213, 31, 161, 55, 134, 6, 7, ..., 133, 5
            1 = 0
            ) = 0
                                        12 (1
            for idx = 0 to length (p) -1:
                  i = (i+1) % 286

j = (j+8[i] % 286

Swap (8[i], 8[j])
                   t = (s[i] + s[j] mod 256
           u = S(E) ([15]8.[8
             and
   * i = 0 j = 0 = ( [ ( j + (s[i]) % 256 ) )
      i = (i+1) % 256 = (0+5(1) % 256
        = (0+1) % 256 = (0 + 213) % 256
                                = 213 020 30 95
      Swap (s[i], s[i]) ([ss]) ([s]) qows
BE - 10 25wap (S[1], S.[213]) MEL 23 181 18 2104 2113 = 3
      t = (S[i] + S[j] % 256
        = (S[213] + S[1] % 256
        = (213+1) % 256
        = 214
      u = s(t)
        ; 5 (214)
      C = U & P(0) = 214 $ 2
         = 11010110
         00000010
                               chr
          11010100 -P 212 -P 0
```

```
* i = 1 , j = 213
                        j = (j + s [i] % 256
   i = (i+1) % 256
    = (1+1) % 256
                         = (213 + 5[2]) % 256
    = 2
                           = (213 + 71) % 256
                           = 284 % 256 = 20
    Swap (s [i], s [i])
    Swap (S[2], S[28])
   t = (s[i] + s[j] % 256
     = (S[28] + S[2] % 256
     = [71+28] % 256
     = 99 % 256
     = 99
    a = S[t]
    = 5 [99]
    C: U & P[1]
      = 99 0 P[1]
      = 9 0 0
      = 01100011
        000000000
        01100011
                      →7 99 : °C "
*i=2,j=28
                         J= (j+S[i]) % 286
  i = (i+1) % 256
                          = (28 + 5[3] % 256
    = (2+1)% 256
                           = (28 + 191) % 256
    = 3
                           = 219
      swap (S[i], S[i])
      swap (SC3], S (219])
   t: (S[i] + S[j] % 256
     = (S [219] + S[3]) % 256
                                 C = U + P[2]
     = (219 + 191) % 256
                                   = 159 0 2
                                   = 1 00 11 0 10
      = 410 % 256
                                    00000010
     = 154
                                     10011000 + 152:"["
   u = SCEJ
      = 5 [154
```