```
ers : 121 + 12 and tradth (6)) and
 Nama: Dw. Hikmah Ramadhani
                                                the eart ecal med sec
  NIM : E1E1 2000 6
                                                     210 1 (27) 4 1 216)
  Kelas: Genap
                                                        (215 + 115 ) mol 256
 Mattul: Kriptografi
                                                         000 born 708
            Soal
1. Kerjakan soar dengan metode ksa dan PGRA, Plaintext nim (4 angka) dan kunci
   (saputra 1)
                               tops (11 + 11 s) + (1 s mod temper (max)) mod acc
             Penyelesaian:
      Array 5: [0,1,2,3,4,5,6,7,8,9,10,...,20,23,24,...,245,246,247,248.
               249,250, 251, 252, 253, 254, 255, 256]
                                                              12 1-50 101
    Dik :
     K = Saputra 1
     Ko= 5
              = 115
     k, = a
               = 97
                                 : (1912 514] of LA mod (smath (M)) mod 215
     k2 = P
                                           : (191 + 4 + 1 (17) mod occ
      K3= U
                                                    200 Poin ((3) 1 40))
     K4: t
                                                    गरेड मेटाम ( अम + रहा)
      Ks +
                                                            THE HOM HE
      ko = a
      k7:1
                                                            (133) 2 (1) 1 : maus
     1=0 1=0/i pertama
     7: ( ] + 5 [i] + k [i & mod Length ( k) ]) mod 256 depart of an 2 ] + (2) 2 + (2)
    Ju)= (0+ 5(0) klo mod length (8) ]) mod 256
                                                       see born ( [ 7] 1 +,00) =
        = (0+0+k[5]) mod 256
                                                        (60+ H4) mod 250
        = (0+k[115])mod 256
                                                             var tour BFJ
      = 115 mod 256 = 115
   Swap = (Stij. S(j))
                                                       (5[6], 5[194])
   swap = (5[0]. 5[115])
  Jus = (115 + 5612 + k[1 mod length (0)]) mod 256
                                          222, hoin ( 12) 4 + 2 + 1+11)
       = (11s+1+k[1]) mod 256
       = (116+ k (a)) mod 256
                                                     100 + [ [ m] ] mod 250
       = (116+ 97) mod 256
                                                        DIS for ( FF + 081)
       = 213 mod 250
       = 213
  Swap = (5[1],5[213])
```

```
J(2) = (213 + 5[2] + k[2 mod Length (8)]) mod 256
    = (213 4 2+k 6[2]) mod 256
    " (215 + k (p1) mod 256
    = (215 + 112) mod 256
    = 327 mod 256
   = 71
 Swap = [5(2), 5(71)]
J(3) = (71 + 5[3] + k [3 mod length (8)]) mod 256
 = (74 + R(u3) mod 256 | 1020 202 pag are 1020 122 122 122 122
  = (74 + 117) mod 256
   = 191 mod 256
 = 191
Swap : [ $(3), $(191)]
J4) = (191+514] + k (4 mod length (8))) mod 256
    = (1g1 + 4 + 1(41) mod 256
    = (1gs + k(k)) mod 256
     = (195 + 116) mod 256
    = 311 mod 256
    = 55
swap = [5(4),5(56)]
Jis) = (55 + 5(5) + k (5 mod length (8)]) mod 256
    = (55 + 5 + k[5]) mod 256 met hom (1 (1) deput hom of 1 (1) 40)
    = (60 + k[r]) mod 256
                                 and Join (1911)
    = (60+ 114) mod 256
     = 174 mod 256
    = 174
swap = (5[6], 5[174])
J(6) = (174 + 5 (6) + k [6 mod length (8)]) mod 256
    : (179+6+ k [6]) mod 256
    = (180+ k[a]) mod 256
                                     (mes le (a)) mod see
    = (180 + 97) mod 256
                                         212 Day (20 4 20)
    = 297 mod 256
    = 21
swap = (5 [6], 5[21])
```

Scanned with CamScanner

= (21 + 5(7) + k (7 mod length (8))) mod 256 = (21+7+k[7]) mod 256 1 e- (i+i) mod 2st : ([+1] med 2s6 = 2 = (28 + k[1]) mod 25c 12 hom (11)2+1) -> 1 = (28 + 49) mod 256 222 | mon ([2] 2 + 5 12) -> = 77 mod 256 1 078 hord (18 + 618) -> = 77 swap = (5[7], 5(77)) Bre Ste how Alic -s For (138) (1) (1) (1) (1) (1) (1) (1) (1) sehingga s=[115, 213, 71, 191, 55, 174, 21, 77, 8, 9, 10, 245, 246, 247, 248, 249, 255 pan [1] 5 + [1] 5 250, 251, 252, 253, 254, 255] 322 hom [82] + [212.5

Laturan Herasi hinggo Herasi te-255, schingga:

S = [115, 213, 71, 191, 55, 174, 21, 77, 255, 105, 71, 44, 211, 101, 150, 244, 93, 207 121, 129, 59, 194, 79, 119, 35, 34, 39, 13, 156, 2, 14, 99, 165, 187, 186, 118, 6, 113, 169, 171, 15, 97, 255, 154, 250, 32, 57, 8, 117, 106, 104, 29, 3, 143, 64 100, 42, 18, 30, 54, 9, 7, 196, 0, 173, 242, 205, 78, 137, 133, 249, 176, 87, 83, 194, 204, 22, 40, 132, 146, 233, 193, 195, 189, 89, 96, 212, 159, 103, 28, 23, 124, 230, 236, 188, 72, 85, 82, 164, 46, 225, 114, 56, 247, 192, 86, 142, 123, 1, 181, 149, 116, 215, 227, 198, 131, 231, 184, 177, 36, 76, 180, 107, 136, 140, 251, 127, 95, 7, 51, 66, 259, 158, 102, 237, 98, 69, 226, 26, 191, 38, 138, 139, 122, 16, 62, 19, 77, 220, 153, 33, 152, 154, 9, 161, 21, 216, 232, 248, 88, 148, 209, 228, 218, 175, 199, 53, 15155, 170, 243, 234, 91, 166, 52, 239, 197, 183, 175, 199, 53, 155, 178, 243, 234, 91, 166, 52, 239, 197, 183, 254, 65, 157, 12, 120, \$70, 224, 197, 60 222, 108, 61, 160, 48, 14, 41, 126, 190, 68, 125, 145, 27, 151, 163, 128, 233, 203, 185, 45, 252, 92, 170, 172, 246, 63, 210, 238, 75, 201, 81, 182, 219, 162, 221, 110, 167, 111, 253, 179, 206, 245, 43, 241, 58, 20, 219, 55, 67, 135, 37, 29, 109, 10, 4, 168, 141, 130, 112, 04, 11, 202, 240, 90, 80,5, 73, 50, 200, 200, 25]

0	404		2 12 4 2 8 mod 208	70
- +	GRA		वार में गार्थ शुरु	
Plantaut 2006			12 =	
Plaintext = 2006		decimal	C1 = 2 C61 = 15	HALL STREET
Index	Value 2	SO	C. C. COp Emdex	
1	0	48	1119 11 11	
2	0	48	पुरः गाम २०२०	
3	6	54	40- can coop	
	_		3000 2011	
Dik: Uneuk			C= 192 5 A	
i=0				
J:0			C = 1 AD	47
index = 0			90 : 6	
		F 2	i (i+1) and 216 = (2+1) mod 215	
1 (i+1) mod 256			35€ (1+2[i]) mod 58€	
J← (j+5[1]			[258 poin (18]3 +0€). →	3
	H. Harris		1 (= (20+191) mod ask	
i ← (0+1) mo	od 256 = 1 me	sd 256 = 1	532 pan 61€ →	
J← (0+ 5[1])		616 ->		
← (0+ 5 [213			(stil, styl) = swap (stal, stal)	
← (0+213) 1			(III, 201, 13, 224, 2, 14,, 18, 19.	
7← 213			see born tyle + till	1
	[1]) = Swap	(5[1],5[213])	335 Powlet 15 + [2]5	
		5, 213, 81,, 2	224 + 310 a od 250	44
		3 mod 256 = 158		100
	8 - nilai da	20 = DOI		
the control of the co		D P[0] = 148 D	(D)	10000
- u by c	maex) = 140 (ש פיףוי נטוץ ע	C = 166 = 1	
			0.100	-
(fater ex)				

```
oze bam (10) digno) bom f 1 4 + (f) 2 + (s)
Untuk 1 = 1
                                                    125 horn ([F] # + F + 12)
     J: 213
                                                        120 + k [[]] mod 250
      i ← (i+1) mod 256 = (1+1) mod 256 = 2
                                                        : (20 + 49) nich 25)
    i ← (j+scij) mod 256
       ← (213+5[2]) mod 256
       ←(213+71) mod 256
                                                            (10f) ? ( 1f12) :
     J - 284 mod 258 = 28
                                                                               20002
swap (5[i], 5[j]) = swap (5[2], 5[28])
   S = (115, 201, 13, 156, 2, 14, ..., 13, 17, ..., 25) 15, 451, 22, 101, 16, 612, 21) -2 promise
   t: sli] + slj] mod 256
     = 5[2] + 5[28] mod 256
     = 13 + 28 mod 256
                                                               DORA
     = 41 mod 250
     = 41
   U = 5(6]: 15
                                             decimal
   C = U Dp [index]
   : 15 @ P[1]
   15 : 1111 0000
   40 = 0011 0000
       1100 0000
   C = 192 = A
 Untuk 1 = 2
       1: 28
       i ← (i+1) mod 256 = (2+1) mod 256 = 3
       J← (J+s[i]) mod 256
         ← (28+5[3]) mod 256
                                                                1 ( (11) mol 250
       J (28+191) mod 256
                                                               1 (- ( 1 + c [ i ] mod 250
         ← 219 mod 256
                                                   and Low 1 = are born (1+0) -> 1
         ← 21g
swap (s(i), s(j)) = swap (s[3], s[219])
   5 = (115, 201, 13, 224, 2, 14, ..., 13, 17, ..., 25)
   t = S[i] + S[j] mod 256
     = 5[3] + 5 [21g] mod 256
     = 224 + 219 mod 256
     = 187
                        222 = 1101 1110
                                        L: $11) + $( 1) = [201 + 113 ] trod 256 = 158
                           48 - 0011 0000
  U= S[t]=222
                               1110 1110
                                                   U+ ११६३ . १४६ - माध्या त्रेका १९४
                                           C= (1 @ p (mass) - 148 @ p101 - 146
   C= UDP (Index)
                           C = 238 = 1
```

No.:	Date.:
Untuk i = 3	
J= 219	
P=(i+1) mod 256 (3+	1) mod 256 = 4
= (j + sci) mod 250	
= 121g + 5141 mod	256
= (21g+ss) mod 256	
= 274 mod 256	
= 13	
swap (sli], slj]) = swap (sl	[4], 5[(8])
5 = (115,201,13,224,7)	
4 = 5 [i] + 5 [j] mod 256	
= 5 [4] + 5 [18] Mod 256	
= 7 + 18 mod 256	
= 25 mod 256	
= 25	
U = 5[6] = 35	
C = U Dp Lindex]	
= 35 D P[3]	
35 = 0010 0011	
sq = 0011 0110	
0001 0101	
C=21 = NAR	
	(KIKY