			ato.	
A			ate	
Nama : Abdull Amnur				1.2
NIM : E1E120055				
. Kerja KSA dan PRGA	dengan	plaintext	nim de	on lunci
(Saputra 1)				
(7401161)		entropistic living		-24
* Algoritma: Key Sche	duling A	lyorama ((ESA)	
Kunci: * Saputra 1*, le	n (K) =	8	102.103	253.284
Array 5: {0,1,2,3,4,5,6	, + , 0 ,	. , 100, 101,	100110)	/ 20 /) . / !
2.5 s · g		7 7 1 2		
and a series of the series of	0			
* Iterasi pertama => i =	0	10 10		
1 20	11.167	7) mod (756	
=> j=(j + 5 [i] + K [i mod	(en (K)	7) 11000	<i>- - - - - - - - - -</i>	No. of Page 1
=(0+0+ K L0 % 8)) 10 L:	0.6		
= (k[0]) % 256	11.	1-4 1 1/2	1164	119
= (-1/3") % 256 =	> pilai	desimal of		- 10
= 115% 256			to the second	
= (15		24-0-80	1000	
Swap (S[i], S[J])			THERE &	MAN THE STATE OF T
Swap (S[0], S[115]) Array S = [115,1,2,3,4,5	.6,7,	10,111,112,1	13, 114, 4,81	6,117,
Array 5 = [13,1,2,3,4,5]	, 202,20	3, 204, 205,	, 250,	251,252
. ,297 , 254, 2	.55]			
	- F. Albert			
* I terasi ke dua -> i =]	10-40-	St. Carlotte St.	All Markey	
S TO THE WAY TO THE TOTAL STATE OF THE STATE		(1)7) 0,	•	
=>j = (j +s[i] + K[1 % (PA	(K) 5) 10	156	
= (115 + (1) + K L				
= (115 + 1 + k[1	1) % 256	1 4	11 . 11	
= (116 + 24) /01		desimal du	na.	= 94
= (116 + 97) %	256			
= 213 % 256				
= 213				
Swap (5[i], 5[j])	Array 5	=[115, 213, 2,	3,45,6,7,	, 112, 113,
Swap (5[1], 5[213])				212,1,214,
		250,251,29		
		7,10 1211	2 1 2 4	164 9351

	Date
Iteras ke-	19a -> 1 = 2
1 . 20	
=23: () 45	[i] + K[i % (en (h)]) % 256
. (713 45	(2) + 4 [2% B] % 256
2 / 21 3 4	2 + k (2]) % 256
- (1)54	"p") "10 256 => dosional dur "p"=112
- (215+	1m) 6/0 256
= 327 %	256
= 71	
	(1),5(1)
Suran (S[i], S[7i]
Array S	
	[115,213,71,3,4,5,6,7,,69,70,2,72,,112,11
	10,16,, 10, 71, 212, 1, 214, 260, 281
	253,254, 255]
* Items Ke	empor -> 1=3
1=31	(2707 -7123
=>5 = (5 4	9 5 27 1 1 5
= = (7/.	5 [1] + k [1 % (on (k)) % 296
= 2/2/	13/6 07) / 256
- : (74	+ ""\ "\ 0 236
- : 191 %	256 => doginal dar "U"=117
= 191	· ·
Swal (([1], ([1])
Array S.	f 1/5 2/2
	[13], [19]]) [15,213,71, 191, 4,5,6,7,69,70, 2,72,, [12,113,114,0.14]
	212 113, 114, 0, 116, (89, 190, 3, 192, 210, 21)
	212 1,214,, 250, 261, 252, 293, 254, 255 3
Mar	
KKY	

```
Date
* Iterasi leelama -> 1=4
  J = 181
     = () +5 [i] + k[i % (en (k)]) % 256
     = (191 + SA] + K[4% O]) % 256
     = (19174 + KE4I) %28
      = (195 + "+") % 256 => desimpl "f" = 116
      = (195 + 116) % 296
  Swap (5 Ci], 5 Cj
                       F: 1 (-
 Sup (5 [4] 5 [35])
            115,213,71,191,55,5,6,7,8, 53,54. 4,56,57
             --, 69, 70,2,72,73, 163,119,0,116,117,-
             189, 190, 3, 1921, ..., 211, 212, 11+214, ..., 250, 251
             252, 253, 254, 255
* Iterasi Keenam -7 1=5
      = (j+5[i]+ K[i /o len (K)]) % 256
       = (5545[5] + K[5% 8]) % 256
         160 + "1" 1 0/0 256 => Nosimal
       - (60 + 114)% 256
       2 174
           E 115, 213, 71, 191,55, 174, 6, 7, 8, ..., 53,54, 4,86
              57, --, 69, 70, 2, 72, 73, --, 113, 114, 0, 116, 12, -, 172,
              173, 5, 175, 176, -, 189, 190, 3, 192, 193, -, 20, 202
              1,219,215,---, 201291,252,293, 254, 259
   Iterasi Kotusch -> i= 6
     = 174
        (j+g(i) + K[i% (en (k)]) % 256
        (174+5 (6) + K [6 %0]) % 256
                         296 => desimal "a" = 97
       (180 + "a")
        L180 +97) % 256
      = 27 70 256
    1 = 21
24471
```

	Date ;
Pseudo-random Generation Automoton	(PRGA)
1.) itorasi Portana -> ldx=0	\ 1
i = 0	110.1
1 = 0	
10 20 (E) 3 (E) - C 6	125 - 10 (1+1) = 1 K=
i = (i+1) mod 256.	26 28 (14.1) E
= (0+1) mal 256	C =
= 1 mod 256,	
= 1	F
j = (i + 5 [i]) mod 256	
= CO 45 [1] mod 256	<u> </u>
= 213 mod 256	3
61 - 17 - 21/3 1 10 F 35 . C YE 85	
Suit = (5.[i],5[i])	0.0 -1.0
= (5[1] 15[VB])	
420 5	o (Transport 150
Array 9 = [115 / 1/28,191,55, 174,21	,77,8,, 20 6,22,
22 21 20 69, 9, 80,	, TO12,72,77,70,
5 3 3 43 119 n 1	16.1171 1721 (9513,
125 (76) (09, (30,3)	1921 1021
, 250, 251, 252, 253, 25	9, 253
	C11000
=> E = (5[17+5[J]) % 256	100 100 100
= (5[1] + 5[213]) % 296	
= (1 +213)% 296	1617 9 BU 1 3 CE
= 219	ma 190 u
= 5 [214] = 214 => 6 iner 214 =	11010110
3 C = V P Cidx]	v casell
= U & P[0] = U & "2" = 7 Biner "2" = 1100	10 11000
= 110 10 110	16 - 00 B 1 E
00110016	· 10-101
C = """, di dos ruel con prensada	228
a a a o vy rock	920 PAPERLINE

Date:
* Herass Ledia -> ldx =1
1007
J = 2/3
=> i = (i+1) % 256 p) i = (j+5[i])% 256
= (1+1) % 256 = (213 A(I)) % 296
= 2 = (213+71)% 256
= 289 % 256
= 28 Swap (Sti] (S[i])
G-00 1 C (2) C (20)
Arroy S = [115, 1, 20, 191, 55, 174, 21, 77, 8,, 19, 20, 6, 22,
24, 26, 27, 71, 29, 30,, 53, 54, 4, 56, 57,, 6
70, 2, 73, 74, 75, 76, 7, 78,, 113, 114, 0, 116, 117,
17 1 (73,5, 175, 176, -, 189, 190,3, 192, 193
213,214,215,, 250,251,252,253,254,255]
=> E = (5 li] +5 [j]) 6256
= (5 (2) + 5 (20)) % 256
= (28+71)% 256
= 99 % 256
= 99
-> 1, - C [1]
=> U = S[t]
= 5 [99]
= 99 => 6 mer 99- 1100011
=> C = U D P [1dx]
= U DP [I]
= U 10 "0"
= 110000
1100011
110000
1010011
(= "5", Desimen = 83
TANKELIN

No. Date:	
* Itorchi Betiga -> ldx =2	* 1/2
1 = 2 ,	
J = 28	
0 0010	
= (2+1) % 256 = (20+5[3])% 256	
= 3 = (28+191) % 256	
= 20	-
- D - C \ AAI	
Swee (S[i], S[i])	
C (6/37, 6(219])	<u> </u>
1 2 1 4 = [115 . 1.78, 219 cc. 174, 21, 77, 0,, 19, 20, 6.	12,
73 76. 97,71,29,30, 53,34, 4,50	0, 1
60 20 9. 35. 39. 25. 76. 7 70, 771.	4,0
122 173 8 - (75) 176, , (09, 190, 3	, 19
017 1/4 1/6 0/6, 607, 200/11/11	,2
253, 279, 257	_
(((1) 5 (1))% 256	
=> t= (S(i)+ 5[j])% 256	
-(5(3) +5(2/9)) 10 20	
= (219+191) % 256	
= 410 % 2360	_
2 194	_
- 101	
=>U = 5 (t)	
	-
= 5 [154] = 1547 Giver = 10011010	
= 1547) Giver = 10000	
DC = UDP [WY]	_
= UAD [2] = UB "5" = 110101	
1 20 11 00	
= 10011010	
00 U0101 @	J
21 41111	
10101111 = 175	
C= "-", desimal = 175	
Note that the distribution of the second sec	

	No. Date :
# LIBITIST (COOMPCH -> ldx -3	10 10 10 10 14 14 14 14 14 14 14 14 14 14 14 14 14
1 = 3	
6 = 219	
=> (= (i+1) % 256 => 1 = (1 + 5/17)	
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
	1) % 296.
= 4 = (219 +55) o	6 296.
= 18	
2 (0	
Swap (S[i] S[j]) (ST)	The first of the state of the s
Swap (S[4], S[18])	1 : 1 : 1
Array 5= (115, 1, 20, 219, 10, 174, 21, 7	17,0, -1 16,1758,19
20, 6, 72, 123, 124, 15, 26, 6	7,91 (79,30,, 53.
54,4,56,57,69,70, 2,7	3,74,75,76,7,78,
792 (13, 164, 0, 116, 117;	, 172, 193,5, 49,
120, -, 189, 190, 3, 192	193,, 2/2,2/3,
214 , 215, 216 , 218, 218, 1 294, 295]	91, 220,, 283,
630 2° 1011 3	
=2 += 5/17+5/17 66 256	FI Lui F
= 5 [4] +5 [10]) ° 6 256	2012
= (10+95) % 296	<u> </u>
= 73	
7	J. 1 : 10
=) U= 8[1]	
25 [33]	
> 73 => 6mor 73 = 100 1001	300 - 300 -
700 5147	- C A - C - C - C - C - C - C - C - C -
7) (- () (+) P [:(ax]	
= U (P (P 3) = U (P (P 4)	, A
= U (10 lol)	
1001001	2 11 11
1001001	1 4 dosimal = 124
0(101010 -7 62	1 pury 1001 - 121
111100	
	110