		No.
		Date:
NAMA	: ZAHWA DIAH AP	× 7: 215 1: 7 /16 76 3

Date:		
NAMA : ZAHWA DIAH AP & ROSA TELESTA		
NIM 17: EIEI20103 digital transit of First Files		
KELAS : GANJIL MANIFORM TOR 3 ] 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		
JUPUGAN : TEKNIK INFORMATIKA [ ] ] + 5 + 3   5   5   5   5   5   5   5   5   5		
(215 + 10) may 356 35 may 100 5 215) -		
TUGAC 2 KRIDTOGRAFIL RCU & DEST		
TUGAS 2 KRIPTOGRAFII, PCY = 2120) =		
-> Key- Scheduling Algorithm (KSA)		
Runoi = Saputra1 (113) (177) and		
Array 5 = [0,1,2,3,4,5,6.7,8,, 100,101, 102,103, 104, 105,, 251, 252, 253, 254, 255]		
5 1 5 1 5 11 5 11 5 1 5 1 5 5 5 6 35 69 10 6 5 2 11 5 16 5 5 2 11 5 5 11 5 15		
* J: 0 sair: 0:0 53/iteracio 125 215 1115 1 515 115		
J = (J + S[i] + K[i mod length (K)]) mod 256		
: (0+0+ K [0 mod 8]) mod 256=1		
= (-KEOI) mod 256 1 mod 17 = +1) =1		
= (s) mod 256 => nilai desimal dan s = 115		
= 115 mad 256 dee pay ([8] = + E + E) =		
ロリラン 115元 1012年前 1511日 (日本 125 1511日 (日本 115) ·		
sump (S[i], S[j]) are bound (and use):		
= 181 mod 250 ([211]) ([21]) quas		
Array S = [115,1,2,3,4,5,6,7,, 110, 111, 112, 113, 114, 0, 116, 117,, 49, 200, 201, 202, 203, 204,		
205,, 251, 252, 253, 254, 255]		
(COR 12 [3]7 ) 3pm)		
* 11 = 115 1, 1 = 111 / iteras 2 3 5 0 5 2 2 0 10 5 215 31 ] . 1 00016		
The was the set of (1 of S[i] + K [i] mod [length (K)]) and [2560]		
= (115 + S cis + K [ i mod 8]) mod 256		
= (115 + 1 + K [i]) mod 256 2 2000 1 3 = 5 4		
= (116 + a) mod 256 => Mai desinal dan a = 97		
: (116 + 197) mod 256 = 127 + 127 + 121) :		
= 213 mod 256 25 hor (1032 + 1 + 101) =		

31 = 1213 F. Jonate Library & 325 byn ( Swap (S[i], S[]]) swap (5[1], 5[213]) Array S = [115, 213, 2, 3, 4, 5, 6, 7, ..., 111, 112, 133, 114, 0, 116, ..., 210, 211, 1212, 1, 214, 215, ...

250, 251, 252, 253, 254, 255}

1. CESE 1, 118.25 115 518 51 151 152 219 51 S4 20, 2, 2 2 23 Acres 0 W E! 532 FS2 \$52 LS2 20 ... 410 1 515 115

No.	
Date:	

A J = Z13, i = 2 / items 3
J = (J + S[i] + K[i mod length (K)]) mod 256
= (213 + S[2] + K[2 mod & ]) mod 256
$\frac{1}{2}$ + 2 + $\frac{1}{2}$ + $\frac{1}{2}$ \ \frac{1}{2} \ \fr
= (215 + P) mad 256 => Miai desirval dari P = 112
= (215 + 112) mod 256
= 327 mand 256
J = 71 (12) willing A miles 12 - 12 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Array S = [115, 213, 71, 3, 4, 5, 6, 7,, 69, 70, 2, 72, 73,, 112, 113, 114, 0, 116, 117,,
210, 211, 212, 1, 214, 215,, 250, 251, 252, 253, 254, 255}
# J = 71, $i = 3$ / iterais $20$ ([6] and $03$ = 4.
J= (J+ Sci] + E[i mod length (x)]) mod 256
= (71 + S[3] + K [3 mod 8]) mod 256
= (71 + 3 + K[3]) mod 256
= (74 + U) mod 256 => Mai definal dai U= 117
= (74 + 117) mod 256 (2022 mod 2 mod
= 191 mod 256 ((2432 1007) cure
Antion of the total of the thing in the property of the total tota
Swap ([[]], [[]]) 1725 U25 275 275 275 275 275
Swap (5[3], 5[191])
Array S = [ 115, 213, 71, 191, 4,5,6,7,, 69,70,2,72,73,,112,113,114,0,116117,,
189, 190, 3, 192, 193,, 210, 211, 212, 1, 214, 215, 251, 252, 253, 254, 255
32 pun (12 pan 1] = + 103 + 311) :
* J= 191, i= 4 / iteras 5 200 hour (100 21 + 1 = 21)
J= (1+ Sci)+ & [i mod (ength (x))) mod 206
= (191 + S[4] + K[4 mod 8]) mod 256
= (1g1 + 4 + K[4]) mod 256 = 1 = 1 = 1 = 1
= (195 + t) mod 25b => nilai desimal dan t = 116
= (195 + 116) mod 256
= 311 wod 256
. 24 Med 218 - 59 A 20 20 20 20 20 20 20 20 20 20 20 20 20
35 of 250 25 25 25 25 ([[]2, []2]) gam3
([4], [5]) (au)
Array S = [115, 213, 71, 191, 55, 5, 6, 7,, 53, 54, 4, 56, 57,, 69, 70, 2, 72, 73,, 113, 114, 0, 116, 117
189, 190, 3, 192, 193,, 211, 212, 1, 214,, 251, 252, 253, 254, 255]

No.				
Date:				
* J= S5, i= \$ / iteras: 6 (45.21) metagent preparation marcal- blood of				
J = (1 + S[i] + k[i  wod length  (k)])  mod  256				
(55 + S[5] + k [5 wod 8]) wod 256				
(160 + 1114 + 1 [5]) mod 25/2 to the color of	_			
1 220 (160 + 1 ) mod 256 -> niai definal ( == 114	_			
= 174 mod 256	_			
J = 174	5			
Sump (SCiJ, SCJJ)				
flab ([61] 5 [13])				
Array S: [115, 213, 71, 191, 55, 174, 6, 7, 8,, 83, 54, 4, 56, 57, 1, 6g, 70, 2, 72, 73,, 113,				
114,0,116,117,, 172,173,5,175,176,,189,190,3,192,193,, 211, 212, 1, 212	1			
325 215; ( 251, 252; 253, 254, 25c] 325 60 N				
812 = 325 Fem 32 = 13				
# J= 174, i= 6 /iteras 7 (1:20 1:00) gail				
J= (j+ Scij + KEi mod leroth (k)) wood 256 32 axxes				
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				
2				
[225, 122 (180 + 20a) smod 1255 815 515 115 - 561 121 8 27, 031				
= 277 mod 256 AS 1000 (EQUI + EUR) = + +				
J = 21 . 325 by (25) 2 + [1] 2) =				
Swap (scij scjj)				
sump (S[6], S[2])				
Array S = [115, 213, 71, 191, 55, 174, 21, 7,8,, 18,19,20,6,22,23,, 53,54,4,56,57,, 69,70,2				
72,73,, 113,114,0,116,117,, 172,173,5,176, 189,190,3,192,193,,				
211, 212, 1, 214, 215,; 251, 252, 254, 253				
11 2 1-2 / Here 2				
J= (j + Scij + K [i mod length (k)]) mod 286 11				
= (21+5(7]+ K[7 mod 8]) mod 256				
= (21+7+KC7) mod 25h				
= (28 + 1) mod 256 => nrai definal dan 1 = 49				
= (28 + 49) mod 256 = 2 man definal de				
= 77 mod 256				
J = 77				
1 FF ) 2 PAN (   1   1   1   1   1   1   1   1   1				
Sump (S[i], S[i]) => Sump (S[7], S[77])  Array S: [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, 10,, 19, 20, 6, 22, 23, 24,, 53, 54, 4, 56, 57, 58,	_			

189, 190, 3, 192, 193, --, 211, 212, 1,214, 215, ..., 251, 252, 253, 254, 255]

	Date:
→ P <sub>2</sub>	2 1 35 11 4
-> Pseudo-Random Generation Algorithm (	PRGA)
Plainteks = 2103 200 (200 )	Sz Su 4, 56,57, 58,
Acray S. [115, 213, 71, 191, 55, 174, 21, 77,8,9,11	0,1 (0,20,6) 22, 23, 24,
69, 70, 2, 72,73, 74, 75, 76, 7, 78,79,,	113, 114,0, 116, 117,, (72,173, 5, 175, (76,177,,
189, 190, 3, 192, 193,, 218, 212, 1, 21	y, 215, 4., 251, 252, 258, 259, 2033
	922 para libe; :
$\frac{1}{2}$ Idx = 0 / iterasi 1	1 = 124
i = 0	(1.27 1.22) gens
	(rufi) 2 . 1217 ) qui
= → i = ((i + 1) mod 256 12 53 →	13=11 (1+ S[i]) mod 2562
me 1 cm (10: (0+1) mod 256 10 36 25	(1) = 21 (0. + S(1)) mod (1256
= 1 mod 256	20 32 (00+ 0213) moder 256
z <u>1</u>	= 213 mod 256 = 213
Supp (SCi], S[1])	= 20-31 1 1 UF1 - 1 K
Juap ([[1]; [[213]) /3) dional to	men 17 4 + + 12 7 + 1) = 1
Array 5 = [115, 1, 71, 191, 55, 174, 21, 77, 8,9,10]	, 19,20,6, 22,23,24,, 53,54,4,56,57,58,,
	ાંક, ાાપ, ૦, -ાં, ૯, ૧૦, ૦૦, ૧૦, ૧૦, ૧૦, ૧૦, ૧૦, ૧૦, ૧૦, ૧૦
189, 190, 3, 192, 193,, 211, 212, 213, 2	
→ t = (S[i] + S[j]) mod 256	
= (S[1] + S[213) mod 256	7 = 24
= (1 + 213] mod 256	(1135 1133) do U
= 214	(501) (501) Nova
ું છે તે એ ક્ષાયુર માયુર દિક્રી . કદાવક ફે જ લાકો ઉન્દ	
195 195 195 196 [hr.] S 1953 195 195 195 195 195	
= 214 3 biner 214 = 1010	
→ C: U & P [idx]	210 60 4100 61 210 112
	5 Km35 5=1, 15=1.4 %
: U & 2 > biner/12 = 111	
2 110 10 110 Fact / 5 Last 6	
00110010 😝 😂 💆	
11100110 parade born <= 0	
С : ä, di desimalkan wenjad	\$ 171.228 ( ) ( ) + 95 ) :
	235 mad 256
	£\$ = 1.
	NG (2022 [13]) BONG
85 43 95 4 165 85 " Mr 82 W 9 de 61 " 4 6 6 8 E	: [로 하는 55 Her 12 위로 84] : 5 Herly
AH 30 20 20 20 60 00 . AN JUDIU DE 81 . 00 000	
- 1550 ASS 550 RED 1 ST DALFTE	રાદ્વાર ેન્દરાય કે એન પથી
	440

	Date:
$\frac{1}{2}$ idx: 1 / iterasi 2	5 1222 1 1 1 1 1
i = 1	c = 1
J = 713	×10 - 1
→ i= (i+1) mod 256 ->	1 = (1+ S[i]) mod 256 -
== (1+1) mod 256	= (213 + 5[2]) mod 256
= 2 2 mod 256 + (10)	= (213 + 71) mod = 256
· 2 25 200 pin .	= 284 mod 256 =
- 25	= 28
Sup (S[i], S[J])	(13) HE ( ) EAR
( [85] ( [2] )	freight tree in the
Array . S = [115,1,28,191,55,174,21,77,8,9,10,	, 19, 20, 6, 22, 23, 24, 25, 26, 27, 71, 29, 30,, 53, 54,
4, 56, 57, 58,, 69, 70, 2, 72, 73, 71	1,75,76,7, 78, 79,, 113,714,0,116,117,
50, FO - 177, 173, 5, 175, 176, 177,, 189, 190,	3, 192, 193,, 211, 212, 213, 214, 215,, 251, 252,
253, 254, 255]	27 . 72 . 47 . · . CT . 205 . (b)
-> t = ( [ [ ] + [ ] ] ) mod 256	952 ( 201 + 1215 ) = 7 2-
= (S[2] + S[28]) mod 256	c (dam (1512)) - 1833
= (28 + 71) mod 256	
= 99 wod 256	à by: aiv :
<del>-</del> 99	71
→ U = [t]	117/ = 14
= S[gg]	[(3)]]
= 99 => biner 99 = 11000 (1)	150 = 150 de 051 =
$\rightarrow C = U \oplus P[id_{7}]$	[+8] 9 9 U : 1 ↔
· u p [1]	
= U @ 1 => biner 1 = 1100	201 100 K S C C C C C
= 1100011	0 m / 90 )
011 0001	<u>ca 1100</u>
1010010	01010101
C: R, desimal dan R=82	L app in App . E = 0

No.

	Date :
$\frac{1}{4}$ $\frac{1}{4}$ $\frac{1}{2}$ $\frac{1}$	E Tours The Street Street
i = 2	A _ 47
J = 28	315 2 7 9
→ i = (i + 1) mod 256 - 1 <- →	1 = (1:+ 5 [i]) mod 256
(z+1) mod 256	= (28+5[3]) mod 256
= 25 31 modizs 30 3 =	= (28 + 191) mod 256
- 3 820 KANN ARE -	= 219 wod 256
: 28	= 219
Swap (S Eiz, S Ezz)	(7.37, 131) 500
Sup (S[3], S[21g])	(1907) [77]
Array 5: [115, 1, 28; 219, 55, 134, 21, 77, 8,9, 10,	19, 20,6, 22, 23, 24, 25, 26, 27, 71, 29, 30,,
53, 54, 4, 56, 57, 58,, 69, 70, 2, 73,74,	
172, 173, 5, 175, 176, 177,, 189, 190, 3, 19	
191, 220, 221, 251, 752, 253, 254, 256	fair yar ist
-Dt = (Scij + Scjj) mod 256	Jone (1972 - 1992) - 🗦 🗢 📗
= (S[3] + S[219]) mod 25b	
= (219 + 191) mod 256	25 Jan 15 + 20 : 1
= 410 mod 256	ME how 69 -
: 154	6.50 -
-> u = ∫[t]	T+7 7 = 11 4
= S[15Y]	[100] 7
= 15y => biner 15y = 10011010	011 = 100 miles (E 1
→ C = U & P [idx]	[+H] 4 8 10 - 7 4
= 4 P[z]	[1] ( = 0 · ·
= U D O => biner 0 == 110 000	) rand 6 1 3 U =
10011010	j. 353 € 10 €
00110000	a long da
10101010	regardent is
C = 9, desirval dais 9 = 170	1 40 10 1892 2 5 C