Nama : Muhammad Ishak Jaelani

NIM : E1E120042

Mata Kuliah : Kriptografi

Soal

1. Kerja KSA dan PRGA dengan plaintext NIM (2042) dan kunci (saputra1). Tulis di kertas!

2. Buat program RC4 menggunakan python

Jawaban

1. KSA dan PRGA

1) KSA

	Key: Sor	•	1.	Mountake Hode
<u> </u>	index	value	decimal	100 As 20 Co 100 /
	0	5	15	211 = 2 = 01
	1	a	93	61 = 0 = 2/3
	2	9	112	16 = 9 = 20
	3	U	119	101 = W = ed
	4	6	116	192. H. pil
	5	7	. 114	(s . r -174
	6	a	97	113 - 0 - 21
	7	7	AQ	ff I el
	***	44	-	and Waldeline and
	5=6,17	23,45,	6, , 20	54,7255] = (0) = 2
	untuk i	0=9,0=		13=1. (= 5 shodal)
	102 19:-(1)	+ SM1+K1	mod lengt	t1(8) 1) mod 250
	0 2 2 (0+0+K6	[[B bom c	mod 256-
	- (0+ 601	mod 256	11/0/01/
	>	(0+((5))	109 520°	nt (さりする) デ
	2	115 mod	1 256 = 11	S boin di
	Swap (S	(1,503,19	= Swap (Sl	(En)/2, [0]
	5=(115,	1,2,3,	11,0,111,	(6,, 255]
		4	1 . j.	0=1,199 86500
	untuk 1	=1/5=16	Jones Joseph	n 1) d 12 1/2 ()
	324 /20	3+503+4	ili mod let	1) mod 256
	= (115+1+	Kli mod a	11 mod 256

No.:	Date:	
<u>—</u>	=(116 + K(1)) mod 256 - 1 = 1 dusino	
5	(16 + 97) mod 256 121)	
5	22 6007 (213 mod 256 123 1 ALIDI) =	
	swap (S[1], S[1]) = swap (S[1], S[213])	
	5=[115,213,2,3,212,1,214,,255]	HOGA
	\$2 = Q2L bun 116 =	
	untuk 1=2,9=213012. [AB) gone (1912. [18] gone	1
	= (1+5(i)+ K[i mod longth (k)]) mod 256	
	3 = (213+2 + K(2 mod B 1 1 1 mod 256	
	= (215 + K(2)) mod 256 = 1 2=1 modio	18
	025 60 = (215 + 112) mod 256 + (1)2 >) = 1	
	1206-1327 (00d=256) 27(1 + 21-22)	
	swap (SP], S(1) 2500 (SP], S(71)	
	S=((15,213,71,3,/-70,2,72,22,1./255)	
	untak e=3,9=71 01/11/22/10/16/256	The Section
	2 (71+3+ K(3 mod	
	221 62 (74 + K(3)) mod 256 /7 / / 1/2 //)	
	= (74+61) mod 2560 (1+2+51)=	
	= 191 trod 256=191 (D+ 00)	
	Swap (5[1], 5[1]) = Swap (5[3], 5[191])	
	S= [15,213, 71, 191, 4 - 10, 190, 3, 192, - 255]	
	5=(115, 215, 11, (Q1, 25, 19A 21 + 11)=3	are de
0	O. Co., Co., Co., Co., Co., Co., Co., Co.	
KIKY	Never give up winner never stop trying	

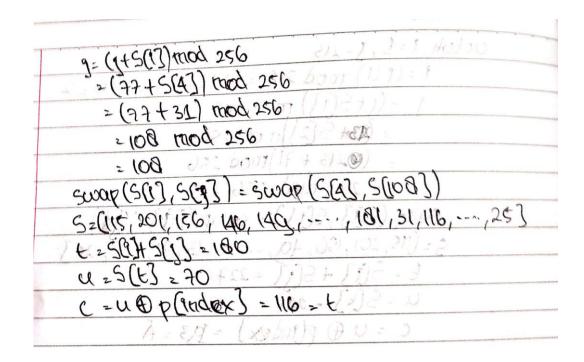
No.:	(12)
	untuk 1 = 4, 9=191 = born ((1)) + 0)1)=
	. (, , < 6.) + K1 mod (onoth(K))) 1000 296
	= (19144 + K/4 mod 30)) 11100 256
	= (195+16(45)) mod 256 (1)= 11)= 1000
	= (105 + (16) mod 256 (215 211) = ?
	= 311 mod 266 = 55
	Swap (S(1), S(2)) = Swap (S(A), S(55)) = 1 HU/OW
	5 2 (15,213) A 1 19 (55,5) - 1,54 A 50 15 - (255)
	be harm U (D) rddors) bost With the stolle I
	untak 1=5, 1=55 = bom (2) + 3/2) -
	1 = (1+5(1) + K(1 mod length (k)) mod 256
	=(55+5+ k(5 mod (256)) mod 256
	= (60+1(4) mod 256= (1)= (1)= (1)= (1)= (1)= (1)= (1)= (1)
	7 (74 mod 256 = 174 - 18 18 21) = 2
	swap (5(1),5(1) = swap(5(5),5(124))
	5 = ((15, 213, 71, 191, 55, 199, 6, +6 -, 173, 5; 175, , 255)
	1 22 POIN (/ (A) 4 DOIN 1) 4 + (1) 5 + () - 1 1 1 1 1 1 1 1 1 1
	untuk 126 (12/14/100) 1001 () 1/ + E+1E)
	9=(9+5(1) + K[1 mod (anoth(K))) mod 256
	= (174+6+ K(6 mod (a) }) mod 256
	= (180 + 97) mod 256 out 10) =
	= 277 mod 256 21212 (102 (102) 90002
	Swap (S(1), S(3)) = Swap (S(6), S(24)) = 814, 21/2
	5=(115, 213,71,191,55,174,21,7,,20,6,22,,255)

No.:
Date:
1=(1+S(1)+K(1) mod (ono+h(k))) mod 201
J=(1+50) + K[1 mod (ength(4))) mod 256
= (201 AC) = 20 20 11 1100 256
$= (20 + 49) \mod 256$ = $17 \mod 256 = 17$
Cump (SG3 CG3) comp (CG3 CG3)
Swap (S[1], S[1]) = swap (S[7], S[77]) 4001
S=[115,213,71,191,55,174,21,77,8,76,7,78,,255]
227
Lakukan Itarasi hinaggi itarasi ka-255, sahinaga:
S=[115, 213, 71, 40, 31, (74, 20, 74, 255, 105, 17, 44, 211, 101,
(10, 214, 3), 201, (21, 124, 14, 14, 14, 14, 14, 14)
11, 12, 10, 10, 10, 10, 11, 11, 11, 11, 11, 11
47,255, 134,250, 32,57,8,117,106,104,20,3,143,64,
100, 42, 10, 30, 54, 0, 7, 106, 0, 173, 242, 205, 78, 137, 138,
240, 46, 41, 121, 201, 140, 10-140, 201, 131
100, 00, 96, 212, 150, 103, 28, 23, 124, 230, 236, 108, 72,
05, 82, 164, 46, 225, (14, 56, 247, 192, 86, 142, 123, 1, 181
(40, 116, 215, 227, 198, 131, 231, 184, 177, 36, 76, 180,
(07, 136, 140, 251, 127, 95, 7, 51, 66, 259, 158, 102, 237, 98, 69, 69, 226, 26, 191, 38, 138, 139, 122, 16, 62, 19, 77, 230
00, 60, 226, 20, 101, 30, 130, 122, 10, 62, 151, 11, 220
(53, 53, 152, 154 a, 161, 21, 216, 237, 48, 88, 148, 200, 228,
218, 175, 198, 53, 155, 178, 243, 234, 91, 166, 52, 230, 197, 183, 254, 65, 157, 12, 120, 190, 224, 147, 60, 222, 108, 61,
(60, 40, 14, 126, 100, 68, 125, 145, 27, 151, 163, 128,
223, 203, (45, 45, 251, 92, 170, 172, 246, 63, 210, 238, 75,
(KKY) One thousand problems, million solution
NOTE TO SELECT THE PARTY OF THE
201, 81, 182, 210, 162, 221, 110, 167, 111, 253, 179, 206, 245, 43, 241, 58, 29, 210, 4, 55, 69, 135, 37, 24, 100, 10, 4, 168, 141, 130, 112, 84, 11, 202, 240, 90, 80, 5, 73,50, 208, 200, 200, 200, 200, 200, 200, 20
(0,4, (68, 141, 130, 112, 84, 11, 202, 240, 90, 80,5,
73,50,208,200,25 100, (2) + (2) =
75,50,000,000,000

2) PRGA

-	plaintaxt	1 2042	55, 194, 22	S= (115, 215, 71 (a),	
	index	volue	decimal		
	Quantity	2,22-07	120,50 040 7	(object the rose t	
1001	多节,到一	0) 01 4	1. (4000	5= (115, 215, 21, 20,	
)हिंदी,	12011	of JAI. 102	, D. 252127 F.	् १५० १४५ ५५, १४	
2)(10)	3:11	2 12 31	1 PUSON 1	0,66,2,4,0	
	. E. DE . AU	1 201 - 111	0,62,40,024	19 19 155 (PA)	
				(UO, 42, Ud 30)	
				mod 256 = 1	16
(J.)	de joe y	+5(93)mod	(760 091 2)	- vc, 00, 000 `	
17 🔃	1,54,00	0+5(1)/10	d 256 201	of Adl ab abe	
(Dir	de +13	(0+213) 7	mod 256	1 100 110 215 2	in the
				COAL OF FOL	
	swapt	(50), 50))= 500 ap (51	1],5(213))	
	5=(115,20	11. 11. 10	,75,213,81	121-121 25 3231	
	ties	[1]+5[1] =	(507 par a	7 (00) (217 , UK) =	
(a)	ec aust	5(4) 214	1800, c, fe	27 90 (AST SP)	
				VA (A), DA, Oo!	
	- 1	Kar Is an			processing the state of the sta

No.:	Date;
	untion 1=1, 1=213 820 6011 (1)2+1) -
	9 = (141) mod 256 = (1+1) mod 256 = 2
	9 = (9+5(1)) mod 256 (10+10) =
	= (2134 S[2] mod 256) 1 DO1 =
	= (243 + 71) mod 256 DO) =
	(100)= 204 mod 256 120 (1)2) your
	swap (S[1], S[1]) = swap (S[2], S[2])
	5=(115,201,156,49,,13,71,42,25)
	t. S(g) + S(g) = 227 Of _ (3) d = 1
	U=S(4) = 241 = (> DDI) y (N -)
	c = U @ p[ndex] = 123 = A
	untak 9=2, 9=28
	P=(1+1) mod 256 = (2+1) mod 256 = 3
	9 = (1+5(93) mod 256
	= (20 + 49) mod 256
	= (77) mod 256 = 99
	Swap (Sfg], S(g]) 2 Swap (S(], Sfg)
	S=(115,201,156,146,31,, 132,40,1233,, 25)
	t=S(?) + 5(1) = 195
	u = S(E) = 145
	C= U @ p[Index] = 165 = \$
	untuk 9=3,9=77
	9 = (9+1) mod 256 (3+1) mod 256 =4
(KI	Y) Never give up, winner never stop trying



2. Program RC4 Enkripsi dan Dekripsi

1) Input Output String

Masukkan PlainText : 2042 Masukkan Kunci Enkripsi : saputra1 ChiperText : ¦Á¥t

Gambar 2. 1 Terminal Program Enkripsi Menggunakan File EncryptionString.py

Masukkan ChiperText : ¦Á¥t Masukkan Kunci Dekripsi : saputra1 PlainText : 2042

Gambar 2. 2 Terminal Program Dekripsi Menggunakan File DecryptionString.py

2) Input Output File



Gambar 2. 3 File input.txt



Gambar 2. 4 File output.txt

Masukkan Nama File PlainText : input.txt Masukkan Nama File ChiperText : output.txt Masukkan Kunci Enkripsi : saputra1

Gambar 2. 5 Terminal Program Enkripsi Menggunakan File EncryptionFile.py

Masukkan Nama File ChiperText : output.txt Masukkan Nama File PlainText : input.txt Masukkan Kunci Dekripsi : saputra1

Gambar 2. 6 Terminal Program Dekripsi Menggunakan File DecryptionFile.py