Mata Kuliah : Kriptografi

Jawablah dengan TELITI, BENAR, SINGKAT dan JELAS. Dilarang menggunakan kalkulator

1. **Soal 1 :** **[Nilai : 25 Poin]**

   Diketahui

   a. Plaintext :
      CF59B416 kunci : E
      Tentukan ciphertext dari plaintext tersebut menggunakan teknik block cipher ECB

   b. Plaintext : A8D7
      Kunci : 4
      IV : 6
      Tentukan ciphertext dari plaintext tersebut menggunakan teknik block cipher CBC

2. **Soal 2 :** **[Nilai : 15 Poin]**

   Jelaskan tentang isu dan solusi yang menjadi perdebatan kontroversial menyangkut keamanan algoritma DES.

3. **Soal 3 :** **[Nilai : 15 Poin]**

   Buatlah table macam-macam varian AES dilengkapi dengan panjang kunci, ukuran blok dan jumlah putarannya.

4. **Soal 4 :** **[Nilai : 30 Poin]**

   Seorang anggota agen badan intelegen CIA akan mengirim pesan berupa **"dei"** menggunakan algoritma RSA, dengan diketahui :
   p = 5 dan q = 7,
   e = 5 → yang merupakan bilangan relatif prima dengan hasil (p-1)(q-1)= (n)

   Tentukan kunci publik & kunci privatnya terlebih dahulu,
   Lalu konversikan pesan plainteks tersebut ke ASCII (sesuai table di bawah ini). Hasil konversi ke ASCII, pecahlah blok plaintext tersebut menjadi 2 digit lalu tentukan hasil akhir cipherteksnya.

Gambarkan diagram proses verifikasi watermarking.

TABEL ASCII

0	32		64	@	96	‘	128	160		192	À	224	à
1	33	!	65	A	97	a	129	161	¡	193	Á	225	á
2	34	"	66	B	98	b	130	162	¢	194	Â	226	â
3	35	#	67	C	99	c	131	163	£	195	Ã	227	ã
4	36	$	68	D	100	d	132	164	¤	196	Ä	228	ä
5	37	%	69	E	101	e	133	165	¥	197	Å	229	å
6	38	&	70	F	102	f	134	166	¦	198	Æ	230	æ
7	39	’	71	G	103	g	135	167	§	199	Ç	231	ç
8	40	(	72	H	104	h	136	168	¨	200	È	232	è
9	41	)	73	I	105	i	137	169	©	201	É	233	é
10	42	*	74	J	106	j	138	170	ª	202	Ê	234	ê
11	43	+	75	K	107	k	139	171	«	203	Ë	235	ë
12	44	,	76	L	108	l	140	172	¬	204	Ì	236	ì
13	45	–	77	M	109	m	141	173	-	205	Í	237	í
14	46	.	78	N	110	n	142	174	®	206	Î	238	î
15	47	/	79	O	111	o	143	175	¯	207	Ï	239	ï
16	48	0	80	P	112	p	144	176	°	208	Đ	240	ð
17	49	1	81	Q	113	q	145	177	±	209	Ñ	241	ñ
18	50	2	82	R	114	r	146	178	²	210	Ò	242	ò
19	51	3	83	S	115	s	147	179	³	211	Ó	243	ó
20	52	4	84	T	116	t	148	180	´	212	Ô	244	ô
21	53	5	85	U	117	u	149	181	µ	213	Õ	245	õ
22	54	6	86	V	118	v	150	182	¶	214	Ö	246	ö
23	55	7	87	W	119	w	151	183	·	215	×	247	÷
24	56	8	88	X	120	x	152	184	¸	216	Ø	248	ø
25	57	9	89	Y	121	y	153	185	¹	217	Ù	249	ù
26	58	:	90	Z	122	z	154	186	º	218	Ú	250	ú
27	59	;	91	[	123	{	155	187	»	219	Û	251	û
28	60	<	92	\	124	|	156	188	¼	220	Ü	252	ü
29	61	=	93	]	125	}	157	189	½	221	Ý	253	ý
30	62	>	94	^	126	~	158	190	¾	222	Þ	254	þ
31	63	?	95	_	127		159	191	¿	223	ß	255	ÿ

Jawablah dengan TELITI, BENAR, SINGKAT dan JELAS. Dilarang menggunakan kalkulator

1. **Soal 1 :** **[Nilai : 25 Poin]**

   Diketahui
   a. Plaintext :
      DB74F329 kunci : A
      Tentukan ciphertext dari plaintext tersebut menggunakan teknik block cipher ECB
   b. Plaintext : E5C8
      Kunci : 3
      IV : 7
      Tentukan ciphertext dari plaintext tersebut menggunakan teknik block cipher CBC

2. **Soal 2 :** **[Nilai : 15 Poin]**

   Gambarkan skema global dari algoritma DES disertai dengan keterangan prosesnya

3. **Soal 3 :** **[Nilai : 15 Poin]**
   Jelaskan spesifikasi algoritma Rijndael.

4. **Soal 4 : RSA sulit** **[Nilai : 30 Poin]**

   Seorang anggota agen badan intelegen CIA akan mengirim pesan berupa **"die"** menggunakan algoritma RSA, dengan diketahui :
   p = 5 dan q = 7,
   e = 5 → yang merupakan bilangan relatif prima dengan hasil (p-1)(q-1)= (n)

   Tentukan kunci publik & kunci privatnya terlebih dahulu,
   Lalu konversikan pesan plainteks tersebut ke ASCII (sesuai table di bawah ini). Hasil konversi ke ASCII, pecahlah blok plaintext tersebut menjadi 2 digit lalu tentukan hasil akhir cipherteksnya.

5. Soal 5 : **[Nilai : 15 Poin]**

Jelaskan perbedaan LSB dan EoF.

TABEL ASCII

0	32	64 @	96 ‘	128	160	192 À	224 à
1	33 !	65 A	97 a	129	161 ¡	193 Á	225 á
2	34 "	66 B	98 b	130	162 ¢	194 Â	226 â
3	35 #	67 C	99 c	131	163 £	195 Ã	227 ã
4	36 $	68 D	100 d	132	164 ¤	196 Ä	228 ä
5	37 %	69 E	101 e	133	165 ¥	197 Å	229 å
6	38 &	70 F	102 f	134	166 ¦	198 Æ	230 æ
7	39 ’	71 G	103 g	135	167 §	199 Ç	231 ç
8	40 (	72 H	104 h	136	168 ¨	200 È	232 è
9	41)	73 I	105 i	137	169 ©	201 É	233 é
10	42 *	74 J	106 j	138	170 ª	202 Ê	234 ê
11	43 +	75 K	107 k	139	171 «	203 Ë	235 ë
12	44 ,	76 L	108 l	140	172 ¬	204 Ì	236 ì
13	45 −	77 M	109 m	141	173 -	205 Í	237 í
14	46 .	78 N	110 n	142	174 ®	206 Î	238 î
15	47 /	79 O	111 o	143	175 ¯	207 Ï	239 ï
16	48 0	80 P	112 p	144	176 °	208 Ð	240 ð
17	49 1	81 Q	113 q	145	177 ±	209 Ñ	241 ñ
18	50 2	82 R	114 r	146	178 ²	210 Ò	242 ò
19	51 3	83 S	115 s	147	179 ³	211 Ó	243 ó
20	52 4	84 T	116 t	148	180 ´	212 Ô	244 ô
21	53 5	85 U	117 u	149	181 µ	213 Õ	245 õ
22	54 6	86 V	118 v	150	182 ¶	214 Ö	246 ö
23	55 7	87 W	119 w	151	183 ·	215 ×	247 ÷
24	56 8	88 X	120 x	152	184 ¸	216 Ø	248 ø
25	57 9	89 Y	121 y	153	185 ¹	217 Ù	249 ù
26	58 :	90 Z	122 z	154	186 º	218 Ú	250 ú
27	59 ;	91 [	123 {	155	187 »	219 Û	251 û
28	60 <	92 \	124 |	156	188 ¼	220 Ü	252 ü
29	61 =	93]	125 }	157	189 ½	221 Ý	253 ý
30	62 >	94 ^	126 ~	158	190 ¾	222 Þ	254 þ
31	63 ?	95 _	127	159	191 ¿	223 ß	255 ÿ