

# Diklat HMIF

# 2017

Database Soal

PAC325

# Kriptografi

Pil. Ganjil



**DAFTAR ISI**

DAFTAR ISI.....	2
SOAL LATIHAN 2009/2010 .....	3
KUIS KRIPTOGRAFI.....	4
UJIAN AKHIR SEMESTER 2011/2012.....	5
UJIAN AKHIR SEMESTER 2012/2013.....	7
UJIAN TENGAH SEMESTER 2013/2014.....	9
UJIAN AKHIR SEMESTER 2013/2014.....	10
UJIAN TENGAH SEMESTER 2014/2015.....	14
UJIAN AKHIR SEMESTER 2014/2015.....	15
UJIAN TENGAH SEMESTER 2015/2016.....	19
UJIAN AKHIR SEMESTER 2015/2016.....	20
UJIAN TENGAH SEMESTER 2016/2017.....	21
UJIAN AKHIR SEMESTER 2016/2017 .....	22

## **SOAL LATIHAN 2009/2010**

1. Diberikan sebuah pesan berikut

P : JANGAN ENGKAU TANGISI MASA MUDAMU YANG TELAH LEWAT TETAPI MENANGISLAH JIKA ENGKAU TIDAK SIAP MENGHADAPI MASA TUAMU

Tentukan tahapan untuk mengenkripsi dan mendekripsi kembali pesan di atas dengan menggunakan teknik vigenere dengan mengambil kunci nama saudara masing-masing.

2. Asumsikan saudara sebagai seorang kriptanalisis, dan pecahkan kode berikut ini.

ECTISAZWWFQGTMAZSWFGUPVNDTOXFGPPRUTBTUZQU

Petunjuk : Gunakan segala kemungkinan untuk memecahkan kode di atas, termasuk analisa frekuensi, cesar chipper dan sebagainya.

# KUIS KRIPTOGRAFI

## KUIS KRIPTOGRAFI

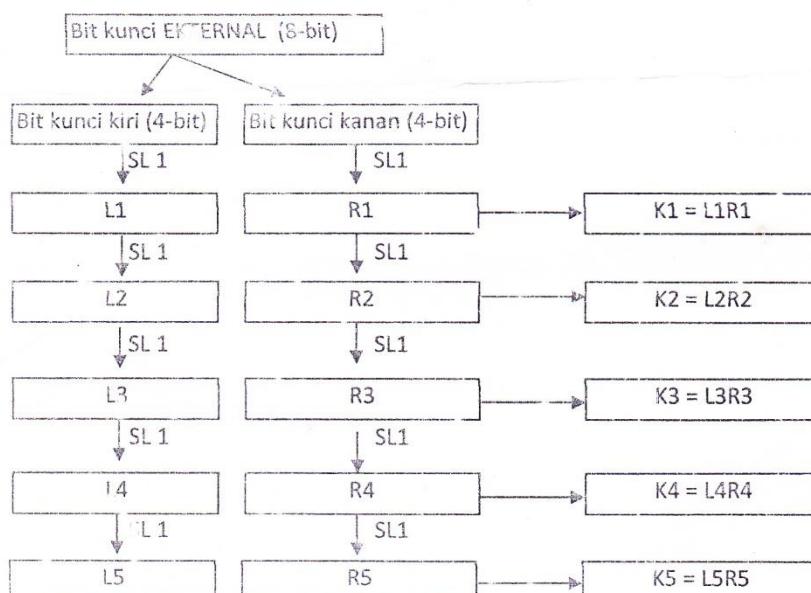
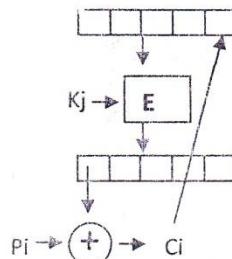
Diketahui suatu data akan dienkripsi dengan sistem berikut:

Metode yang digunakan adalah CFB 8-bit dengan panjang blok 40 bit tiap blok (setiap blok akan mempunyai 5 blok kecil berukuran 8-bit) dengan menggunakan kunci yang dihasilkan oleh suatu keystream generator dan setiap blok kecil menggunakan kunci yang berbeda sesuai dengan indeks blok kecil tersebut. Fungsi Enkripsi E didefinisikan sebagai:

1. Geser kiri antrian sejauh 2
2. (Hasil langkah satu) XOR Kj
3. Geser ke kanan (hasil langkah kedua) sejauh 1
4. (Hasil langkah ketiga) XOR Kj

IV yang digunakan adalah "HARUS"

Adapun Keystream generator yang digunakan adalah



Enkripsi kalimat "KERJAKAN DENGAN BENAR" dengan kunci eksternal "Z" dengan asumsi spasi tidak diperhatikan

Tabel ASCII

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F	50	51	52	53	54	55	56	57	58	59	5A

# UJIAN AKHIR SEMESTER 2011/2012



Ujian Akhir Semester Ganjil 2011/2012  
 Program Studi Informatika  
 Jurusan Matematika FMIPA UNDIP Semarang

---

Mata Kuliah	:	KRIPTOGRAFI
Sifat	:	Open Book
Waktu	:	90 Menit

---

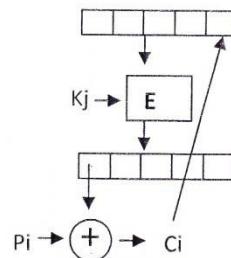
Diketahui suatu data akan dienkripsi dengan sistem berikut:

Metode yang digunakan adalah **CFB 8-bit** dengan panjang blok 40 bit tiap blok (setiap blok akan mempunyai 5 blok kecil berukuran 8-bit) dengan menggunakan kunci yang dihasilkan oleh suatu keystream generator dan setiap blok kecil menggunakan kunci yang berbeda sesuai dengan indeks blok kecil tersebut. **Fungsi Enkripsi E** didefinisikan sebagai:

1. Geser kanan antrian sejauh 2
2. (Hasil langkah satu) XOR  $K_j$
3. Permutasi hasil langkah 2 dengan TABEL PERMUTASI di bawah ini

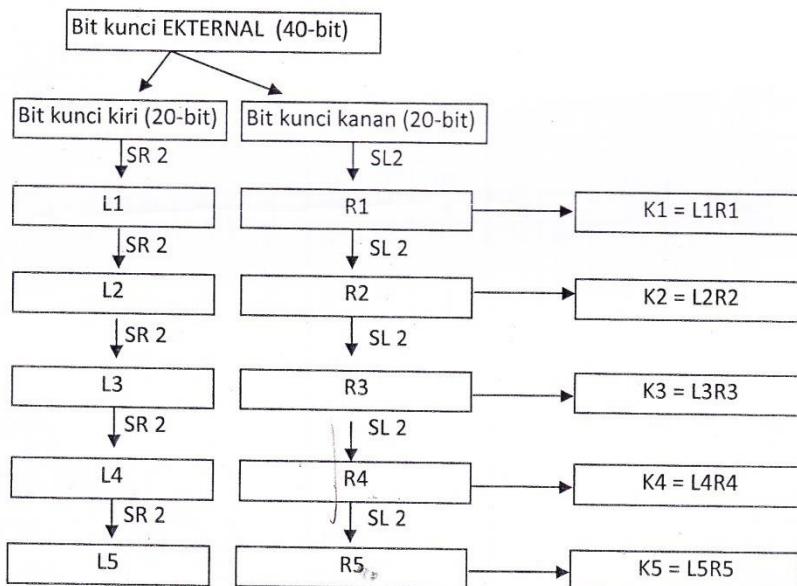
**Tabel PERMUTASI**

17	18	19	20	21	22	23	24
9	10	11	12	13	14	15	16
8	7	6	5	4	3	2	1
25	26	27	28	29	30	31	32
40	39	38	37	36	35	34	33



IV yang digunakan adalah "HARUS"

Adapun Keystream generator yang digunakan adalah

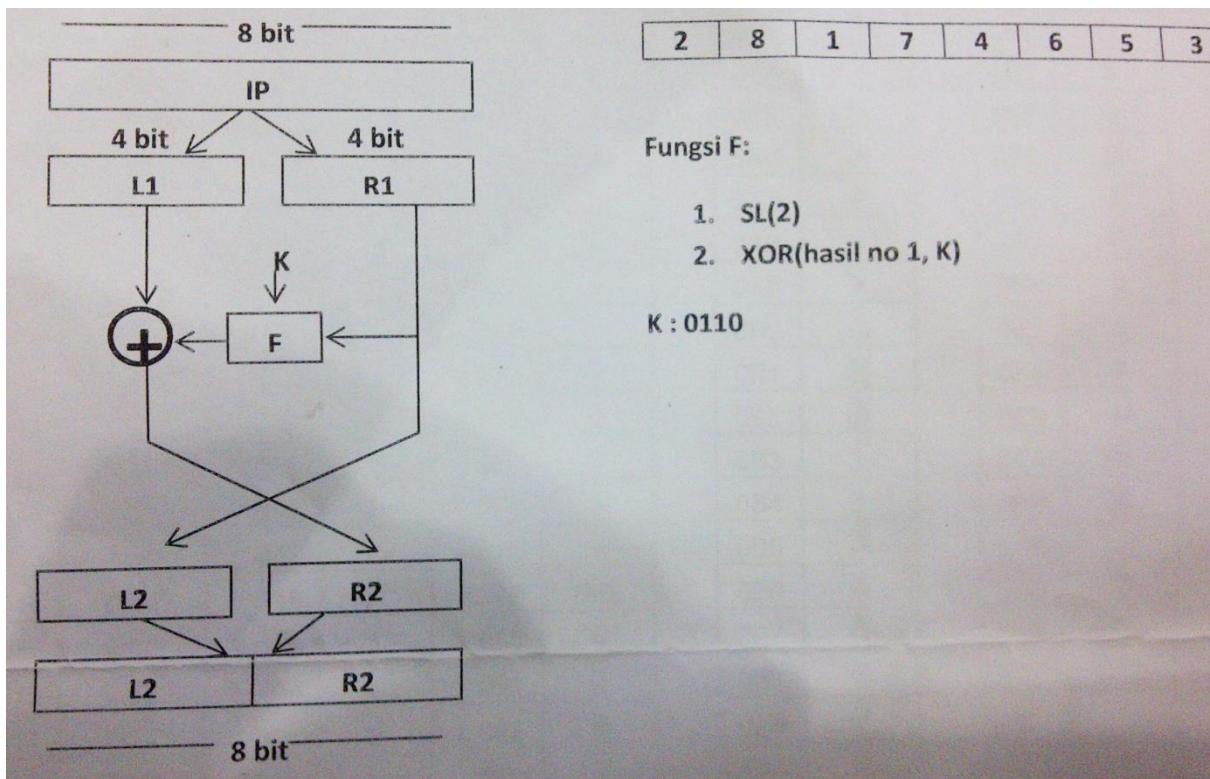


Cari kunci yang dihasilkan kemudian enkripsi kalimat "KERAS" dengan kunci eksternal "MUDAH" dengan asumsi spasi tidak diperhatikan! BERIKAN KUNCI DAN CHIPERTEXT DALAM BENTUK ALFABET!

TABEL ASCII

DEC	HEX	Symbol															
0	00	NUL	47	2F	/	94	5E	^	141	8D		188	BC	¼	235	EB	ë
1	01	SOH	48	30	0	95	5F	-	142	8E	Ž	189	BD	½	236	EC	ì
2	02	STX	49	31	1	96	60	,	143	8F		190	BE	¾	237	ED	í
3	03	ETX	50	32	2	97	61	a	144	90		191	BF	đ	238	EE	î
4	04	EOT	51	33	3	98	62	b	145	91	'	192	C0	À	239	EF	ï
5	05	ENQ	52	34	4	99	63	c	146	92	"	193	C1	Á	240	F0	ð
6	06	ACK	53	35	5	100	64	d	147	93	"	194	C2	Â	241	F1	ñ
7	07	BEL	54	36	6	101	65	e	148	94	"	195	C3	Ã	242	F2	ò
8	08	BS	55	37	7	102	66	f	149	95	*	196	C4	Ä	243	F3	ó
9	09	HT	56	38	8	103	67	g	150	96	-	197	C5	Å	244	F4	ô
10	0A	*LF	57	39	9	104	68	h	151	97	-	198	C6	Æ	245	F5	ð
11	0B	VT	58	3A	:	105	69	i	152	98	~	199	C7	Ç	246	F6	ö
12	0C	FF	59	3B	;	106	6A	j	153	99	™	200	C8	È	247	F7	÷
13	0D	CR	60	3C	<	107	6B	k	154	9A	š	201	C9	É	248	F8	ø
14	0E	SO	61	3D	=	108	6C	l	155	9B	›	202	CA	Ê	249	F9	ù
15	0F	SI	62	3E	>	109	6D	m	156	9C	œ	203	CB	Ë	250	FA	ú
16	10	DLE	63	3F	?	110	6E	n	157	9D		204	CC	Ì	251	FB	û
17	11	DC1	64	40	@	111	6F	o	158	9E	ž	205	CD	Í	252	FC	ü
18	12	DC2	65	41	A	112	70	p	159	9F	Ý	206	CE	Î	253	FD	ý
19	13	DC3	66	42	B	113	71	q	160	A0		207	CF	Ï	254	FE	þ
20	14	DC4	67	43	C	114	72	r	161	A1	í	208	D0	Ð	255	FF	ÿ
21	15	NAK	68	44	D	115	73	s	162	A2	ć	209	D1	Ñ			
22	16	SYN	69	45	E	116	74	t	163	A3	£	210	D2	Ò			
23	17	ETB	70	46	F	117	75	u	164	A4	¤	211	D3	Ó			
24	18	CAN	71	47	G	118	76	v	165	A5	¥	212	D4	Ô			
25	19	EM	72	48	H	119	77	w	166	A6	¦	213	D5	Õ			
26	1A	SUB	73	49	I	120	78	x	167	A7	§	214	D6	Ö			
27	1B	ESC	74	4A	J	121	79	y	168	A8	"	215	D7	×			
28	1C	FS	75	4B	K	122	7A	z	169	A9	©	216	D8	Ø			
29	1D	GS	76	4C	L	123	7B	{	170	AA	ª	217	D9	Ù			
30	1E	RS	77	4D	M	124	7C		171	AB	«	218	DA	Ú			
31	1F	US	78	4E	N	125	7D	}	172	AC	¬	219	DB	Û			
32	20	spasi	79	4F	O	126	7E	~	173	AD	-	220	DC	Ü			
33	21	!	80	50	P	127	7F	DEL	174	AE	®	221	DD	Ý			
34	22	"	81	51	Q	128	80	€	175	AF	-	222	DE	Þ			
35	23	#	82	52	R	129	81		176	B0	°	223	DF	ß			
36	24	\$	83	53	S	130	82	,	177	B1	±	224	E0	à			
37	25	%	84	54	T	131	83	f	178	B2	²	225	E1	á			
38	26	&	85	55	U	132	84	"	179	B3	³	226	E2	â			
39	27	'	86	56	V	133	85	...	180	B4	'	227	E3	ã			
40	28	(	87	57	W	134	86	†	181	B5	µ	228	E4	ä			
41	29	)	88	58	X	135	87	‡	182	B6	¶	229	E5	å			
42	2A	*	89	59	Y	136	88	^	183	B7	.	230	E6	æ			
43	2B	+	90	5A	Z	137	89	%	184	B8	,	231	E7	ç			
44	2C	,	91	5B	[	138	8A	Š	185	B9	¹	232	E8	è			
45	2D	-	92	5C	\	139	8B	<	186	BA	º	233	E9	é			
46	2E	.	93	5D	]	140	8C	Œ	187	BB	»	234	EA	ê			

# UJIAN AKHIR SEMESTER 2012/2013



1. Jika diketahui suatu chipertext dalam bilangan hexadecimal sebagai berikut: **5C812537F0** dan diketahui juga bahwa mode enkripsi yang digunakan adalah mode **CBC** dengan panjang blok 8 bit, fungsi **E** yang digunakan seperti tampak pada gambar dan keterangan di atas serta **IV: 10101010**, maka cari plaintext dari chipertext tersebut dalam **kode ASCII**!
2. Dengan menggunakan fungsi **E** di atas cari chipertext dari plaintext berikut  
Plaintext : **SEMOGA BERHASIL**  
Dengan ketentuan:  
Gunakan mode **CFB** dengan panjang blok **m=8, n=4**, **IV: 01010101**, spasi tidak diperhitungkan  
Chipertext dalam bentuk bilangan Hexadecimal
3. Diberikan proses ekripsi dan dekripsi untuk stream cipher  

<b>proses enkripsi</b>	<b>proses dekripsi</b>	
$c = (p+k) \bmod 26$	$p = (c-k) \bmod 26$	
dimana:		
$c = \text{ciphertext}$	$p = \text{plaintext}$	$k = \text{kunci}$

  - a. Mungkinkah proses di atas menjadi suatu proses yang **ONE TIME PAD** jelaskan?
  - b. Bila jawaban poin a adalah mungkin, tentukan syarat agar proses di atas menjadi berlaku **ONE TIME PAD**? Bila jawaban poin a adalah tidak mungkin, berikan alasannya!

TABEL ASCII

DEC	HEX	Symbol															
0	00	NUL	47	2F	/	94	5E	^	141	8D		188	BC	¼	235	EB	ë
1	01	SOH	48	30	0	95	5F	-	142	8E	Ž	189	BD	½	236	EC	ì
2	02	STX	49	31	1	96	60	,	143	8F		190	BE	¾	237	ED	í
3	03	ETX	50	32	2	97	61	a	144	90		191	BF	¸	238	EE	î
4	04	EOT	51	33	3	98	62	b	145	91	'	192	C0	À	239	EF	ï
5	05	ENQ	52	34	4	99	63	c	146	92	'	193	C1	Á	240	F0	ð
6	06	ACK	53	35	5	100	64	d	147	93	"	194	C2	Â	241	F1	ñ
7	07	BEL	54	36	6	101	65	e	148	94	"	195	C3	Ã	242	F2	ò
8	08	BS	55	37	7	102	66	f	149	95	•	196	C4	Ä	243	F3	ó
9	09	HT	56	38	8	103	67	g	150	96	-	197	C5	Å	244	F4	ô
10	0A	*LF	57	39	9	104	68	h	151	97	-	198	C6	Æ	245	F5	ð
11	0B	VT	58	3A	:	105	69	i	152	98	~	199	C7	Ç	246	F6	ö
12	0C	FF	59	3B	;	106	6A	j	153	99	™	200	C8	È	247	F7	÷
13	0D	CR	60	3C	<	107	6B	k	154	9A	š	201	C9	É	248	F8	ø
14	0E	SO	61	3D	=	108	6C	l	155	9B	>	202	CA	Ê	249	F9	ù
15	0F	SI	62	3E	>	109	6D	m	156	9C	œ	203	CB	Ë	250	FA	ú
16	10	DLE	63	3F	?	110	6E	n	157	9D		204	CC	Ì	251	FB	û
17	11	DC1	64	40	@	111	6F	o	158	9E	ž	205	CD	Í	252	FC	ü
18	12	DC2	65	41	A	112	70	p	159	9F	Ý	206	CE	Î	253	FD	ý
19	13	DC3	66	42	B	113	71	q	160	A0		207	CF	Ï	254	FE	þ
20	14	DC4	67	43	C	114	72	r	161	A1	í	208	D0	Ð	255	FF	ÿ
21	15	NAK	68	44	D	115	73	s	162	A2	¢	209	D1	Ñ			
22	16	SYN	69	45	E	116	74	t	163	A3	£	210	D2	Ò			
23	17	ETB	70	46	F	117	75	u	164	A4	¤	211	D3	Ó			
24	18	CAN	71	47	G	118	76	v	165	A5	¥	212	D4	Ô			
25	19	EM	72	48	H	119	77	w	166	A6	!	213	D5	Ô			
26	1A	SUB	73	49	I	120	78	x	167	A7	§	214	D6	Ö			
27	1B	ESC	74	4A	J	121	79	y	168	A8	"	215	D7	×			
28	1C	FS	75	4B	K	122	7A	z	169	A9	©	216	D8	Ø			
29	1D	GS	76	4C	L	123	7B	{	170	AA	ª	217	D9	Ù			
30	1E	RS	77	4D	M	124	7C		171	AB	«	218	DA	Ú			
31	1F	US	78	4E	N	125	7D	}	172	AC	¬	219	DB	Û			
32	20	spasi	79	4F	O	126	7E	~	173	AD	-	220	DC	Û			
33	21	!	80	50	P	127	7F	DEL	174	AE	®	221	DD	Ý			
34	22	"	81	51	Q	128	80	€	175	AF	-	222	DE	Þ			
35	23	#	82	52	R	129	81		176	B0	º	223	DF	ß			
36	24	\$	83	53	S	130	82	,	177	B1	±	224	E0	à			
37	25	%	84	54	T	131	83	f	178	B2	²	225	E1	á			
38	26	&	85	55	U	132	84	„	179	B3	³	226	E2	â			
39	27	'	86	56	V	133	85	...	180	B4	°	227	E3	ã			
40	28	(	87	57	W	134	86	†	181	B5	µ	228	E4	ä			
41	29	)	88	58	X	135	87	‡	182	B6	¶	229	E5	å			
42	2A	*	89	59	Y	136	88	^	183	B7	·	230	E6	æ			
43	2B	+	90	5A	Z	137	89	%	184	B8	,	231	E7	ç			
44	2C	,	91	5B	[	138	8A	Š	185	B9	¹	232	E8	è			
45	2D	-	92	5C	\	139	8B	<	186	BA	º	233	E9	é			
46	2E	.	93	5D	]	140	8C	Œ	187	BB	»	234	EA	ê			

## UJIAN TENGAH SEMESTER 2013/2014

Mata Kuliah : Kriptografi

Waktu : 90 menit

M N U U N M X I L U U A C S Q C S I W N V

1. Terdapat sebuah plainteks **ANUGERAH ICT PURA KOTA SEMARANG**. Tentukan cipherteks dari plainteks tersebut, jika digunakan algoritma **playfair** dengan menggunakan kunci nama lengkap saudara masing-masing.
2. Tentukan hasil bilangan random dari  $X_n = (aX_{n-1} + b) \bmod m$ , jika diambil nilai  $a = 5$ ,  $b = 9$ ,  $m = 13$  dan  $X_0 = 0$ . Tentukan pula periode dari bilangan random tersebut.
3. Terdapat cipherteks sebagai berikut :

**R X O X R U R R B M Q A C N Z B I D X X L**

Tentukan plainteks dari cipher di atas, jika diketahui :

- a. Algoritma yang digunakan adalah **super enkripsi**
- b. Kunci yang digunakan salah satunya adalah **nama matakuliah**.

# UJIAN AKHIR SEMESTER 2013/2014



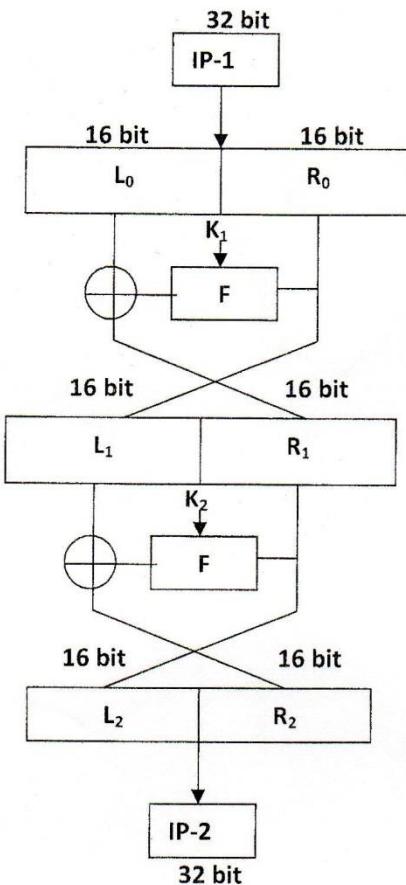
UJIAN AKHIR SEMESTER GASAL 2013/2014  
JURUSAN ILMU KOMPUTER/ INFORMATIKA  
FAKULTAS FSM UNDIP

Mata Kuliah : KRIPTOGRAFI

Waktu : 90 menit

Sifat : Open Book

Fungsi E:



Fungsi F:

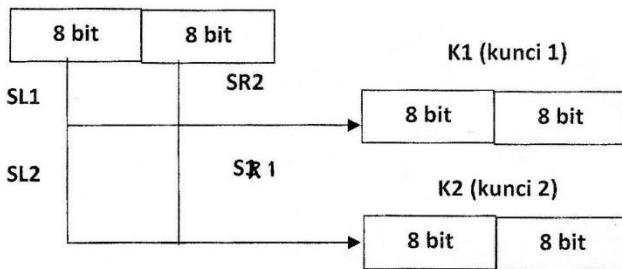
1. SL2
2. Hasil no 1 XOR K

Tabel IP-1

17	19	21	23	24	22	20	18
9	11	13	15	16	14	12	10
8	7	6	5	1	4	3	2
25	26	27	28	29	30	31	32

Tabel IP-2

16	15	14	13	12	11	10	9
8	7	6	5	4	3	2	1
17	18	19	20	21	22	23	24
28	27	26	25	29	30	31	32

**Keystream Generator**

1. Dengan menggunakan skema fungsi enkripsi (**E**) dan Keystream Generator di atas dan menggunakan metode cipher block **ECB dengan panjang blok (m) = 32 bit**, maka cari ciphertext dari plaintext berikut (spasi tidak dianggap) : **COBA DULU**

Ketentuan : gunakan kunci eksternal **AB**

Output (ciphertext) harus dalam bentuk **karakter**, bukan biner dan bukan heksadesimal

2. A. Kapan suatu algoritma enkripsi pada skema stream mengalami kondisi one time pad?

B . diketahui bahwa suatu algoritma stream cipher mempunyai rumus

**proses enkripsi**

$$C = P \text{ xor } K$$

dimana:

$$C = \text{ciphertext} \quad P = \text{plaintext} \quad K = \text{kunci}$$

dengan k dihasilkan oleh Keystream Generator berikut:

Input berupa masukan 6 digit ( ambil 101100)

Kemudian generate kunci dengan cara lakukan operasi XOR antara bit terakhir dengan 5 bit sebelumnya,  $\text{digit}[n+1] = \text{digit}[n] \text{ xor } \text{digit}[n-5]$

Contoh : 101100 maka hasilnya adalah 10110011....

Apakah algoritma yang diberikan di atas akan mengalami kondisi one time pad? Berikan alasan Anda!

3. Jika diketahui suatu fungsi enkripsi sederhana sebagai berikut :

1.  $SL8(P)$
2.  $(1) \text{ xor } SR8(k)$
3.  $SL1(2)$

Dan diketahui juga bahwa suatu plainteks yang dimasukkan menghasilkan suatu ciphertext **h^v** (dalam hex : 68 5E 60) maka :

- a. Tentukan fungsi dekripsinya
- b. cari palintext yang dimaksud (tulis dalam karakter, bukan heksadesimal atau biner) apabila kunci yang diberikan adalah **DIA** (perhatikan huruf kapital atau tidaknya!)

## ASCII TABLE (GUNAKAN 2 DIGIT TERAKHIR DARI NILAI HEX)

027	'
028	(
029	)
02A	*
02B	+
02C	,
02D	-
02E	.
02F	/
030	0
031	1
032	2
033	3
034	4
035	5
036	6

05E	^
05F	-
060	'
061	a
062	b
063	c
064	d
065	e
066	f
067	g
068	h
069	i
06A	j
06B	k
06C	l
06D	m

095	ò
096	û
097	ù
098	ÿ
099	Ö
09A	Ü
09B	ø
09C	£
09D	Ø
09E	×
09F	f
0A0	á
0A1	í
0A2	ó
0A3	ú
0A4	ñ

0CC	Ŀ
0CD	=
0CE	ܵ
0CF	ݏ
0D0	ݔ
0D1	܍
0D2	܎
0D3	܏
0D4	ܐ
0D5	ܑ
0D6	ܒ
0D7	ܓ
0D8	ܔ
0D9	ܕ
0DA	ܖ
0DB	ܗ

## UJIAN TENGAH SEMESTER 2014/2015

SOAL UTS KRIPTOGRAFI

WAKTU : 90 MENIT

SIFAT : TUTUP BUKU

Jawab pada lembar yang telah disediakan.

1. Jika diberikan cipherteks YVEK ZBRE LCRY YRTB VIDR CRPJ ZR, tentukan plainteks yang sesungguhnya.

2. Diberikan sebuah plainteks : BAHAYA VIRUS EBOLA

Gunakan algoritma play fair dengan kunci nama lengkap saudara untuk mengenkripsi plainteks.

3. Cipher Q M G V J I O Y N A R T E U S D C J dienkripsi dengan algoritma *Hill Cipher* menggunakan matriks  $\begin{bmatrix} 6 & 3 \\ 1 & 4 \end{bmatrix}$ . Tentukan isi plainteksnya.

4. Tentukan plainteks dari S N P J I V J D N Q R D X O E O H I G I L N T N V H I W, di mana kunci yang digunakan memiliki panjang 7 karakter.

X H A P V A B R Z C N G N Q N Q V A B G V T N

# UJIAN AKHIR SEMESTER 2014/2015



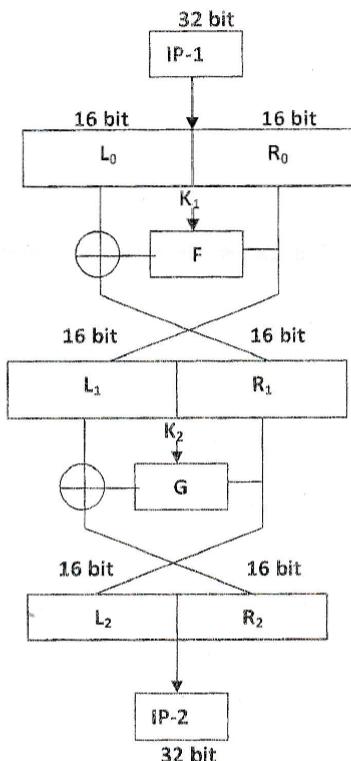
**UJIAN AKHIR SEMESTER GASAL 2014/2015**  
**JURUSAN ILMU KOMPUTER/ INFORMATIKA**  
**FAKULTAS FSM UNDIP**

Mata Kuliah : KRIPTOGRAFI

Waktu : 90 menit

Sifat : Open Book

Fungsi E:



Fungsi F:

1. SL2
2. Hasil no 1 XOR K<sub>1</sub>

Fungsi G:

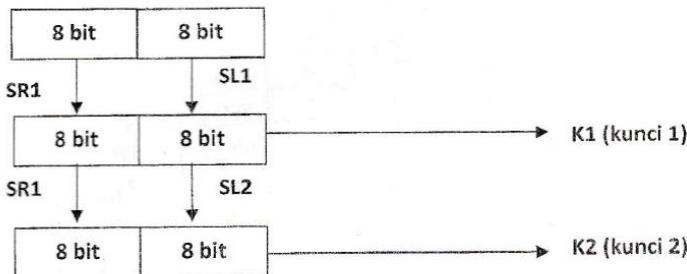
1. SR3
2. Hasil no 1 XOR K<sub>2</sub>

**Tabel IP-1**

17	19	21	23	24	22	20	18
9	11	13	15	16	14	12	10
8	7	6	5	1	4	3	2
25	26	27	28	29	30	31	31

Tabel IP-2

16	15	14	13	12	11	10	9
8	7	6	5	4	3	2	1
17	18	19	20	21	22	23	24
28	27	26	25	29	30	31	32

**Keystream Generator**

1. Dengan menggunakan skema fungsi enkripsi (**E**) dan Keystream Generator di atas dan menggunakan metode cipher block **ECB** dengan panjang blok (**m**) = **32 bit**, maka cari ciphertext dari plaintext berikut (spasi tidak dianggap) : **AKAN COBA**  
 Ketentuan : gunakan kunci eksternal **AH**  
 Output (ciphertext) harus dalam bentuk **karakter**, bukan biner dan bukan heksadesimal

2. A. Kapan suatu algoritma enkripsi pada skema stream mengalami kondisi one time pad?

B . diketahui bahwa suatu algoritma stream cipher mempunyai rumus

$$\text{proses enkripsi} \quad \text{proses dekripsi}$$

$$C = (P + K) \text{ MOD } 2 \quad P = (C + K) \text{ MOD } 2$$

dimana:

$$C = \text{ciphertext} \quad P = \text{plaintext} \quad K = \text{kunci}$$

dengan k dihasilkan oleh Keystream Generator berikut:

Input berupa masukan 6 digit ( ambil 101100)

Kemudian generate kunci dengan cara lakukan operasi XOR antara bit terakhir dengan 5 bit sebelumnya,  $\text{digit}[n+1] = \text{digit}[n] \text{ xor digit}[n-5]$

Contoh : 101100 maka hasilnya adalah 10110011....

Apakah algortima yang diberikan di atas akan mengalami kondisi one time pad? Berikan alasan Anda!

3. Jika diketahui suatu fungsi enkripsi sederhana sebagai berikut :

1.  $\text{SR6}(P)$
2.  $(1) \text{ xor SR2}(K)$
3.  $\text{SL8}(2)$

Dan diketahui juga bahwa suatu plainteks yang dimasukkan menghasilkan suatu ciphertext **Ouh** (perhatikan huruf kapital atau tidaknya!) maka :

a. Tentukan fungsi dekripsinya

b. cari plaintext yang dimaksud (tulis dalam karakter **dan** heksadesimal bukan dalam biner) apabila kunci yang diberikan adalah **DIA** (perhatikan huruf kapital atau tidaknya!)

ASCII TABLE  
(GUNAKAN **2 DIGIT TERAKHIR** DARI NILAI HEX)



027	'
028	(
029	)
02A	*
02B	+
02C	,
02D	-
02E	.
02F	/
030	0
031	1
032	2
033	3
034	4
035	5
036	6

05E	^
05F	-
060	'
061	a
062	b
063	c
064	d
065	e
066	f
067	g
068	h
069	i
06A	j
06B	k
06C	l
06D	m

095	ò
096	û
097	ù
098	ÿ
099	Ö
09A	Ü
09B	ø
09C	£
09D	Ø
09E	×
09F	f
0A0	á
0A1	í
0A2	ó
0A3	ú
0A4	ñ

0CC	॥
0CD	=
0CE	॥
0CF	¤
0D0	ð
0D1	đ
0D2	ê
0D3	ë
0D4	è
0D5	í
0D6	í
0D7	î
0D8	ï
0D9	」
0DA	ؒ
0DB	ؓ

## UJIAN TENGAH SEMESTER 2015/2016



Ujian Tengah Semester Gasal 2015/2016  
Jurusan Ilmu Komputer/ Informatika  
FMIPA UNDIP Semarang

Mata Kuliah	:	Kriptografi	Hari	:	Kamis
Sifat	:	Buku Tertutup	Tanggal	:	5 Nopember 2015
Waktu	:	90 Menit	Jam	:	13.00 – 14.30

1. Diketahui suatu ciphertext diperoleh dengan melakukan proses enkripsi Vigenere dengan kunci berupa nama dari suatu mata kuliah di prodi Ilmu Komputer dan dilanjutkan dengan melakukan operasi transpose dengan kunci = 4-3-5-2-1, apabila diketahui ciphertext yang dimaksud adalah

**MZDXMAMLAEIJJSOMDHMWALKZHHTY! AAAEAL**

maka carilah Plaintextnya!

2. Seorang kriptoanalisis mencoba menemukan plaintext dari suatu ciphertext sebagai berikut

**CYGPDLMHDKCUZQYW霍VMSYK**

apabila dia menemukan bahwa metode yang digunakan untuk mengenkripsi plaintext yang dicari adalah dengan menggunakan Hill Cipher dengan matrik kunci

$$\text{Kunci} = \begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix}$$

maka bantulah kriptoanalisis tersebut untuk menemukan plaintext yang dimaksud!

# UJIAN AKHIR SEMESTER 2015/2016



**KEMENTERIAN RISET, TEKNOLOGI, DAN PENDIDIKAN TINGGI**  
**UNIVERSITAS DIPONEGORO**  
**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM**  
 Jalan Prof. H. Soedarto, SH. Tembalang Semarang 50275;  
 Telp : (024) 7474754; Fax : (024) 76480690; E-mail : mipa@undip.ac.id

## UJIAN AKHIR SEMESTER GASAL 2015/2016

Mata Kuliah	:	Kriptografi
Kelas	:	A & B
Pengampu	:	Helmie Arif Wibawa, M.Cs. / Edy Suharto, S.T.
Jurusan	:	Informatika
Hari / Tanggal	:	Kamis, 14 Januari 2016
Jam / Ruang	:	13.00 – 14.30 WIB (90 menit) / A204, A205
Sifat Ujian	:	Buku terbuka, kalkulator

**Petunjuk Pengerjaan :**

Jawablah soal-soal berikut pada lembar jawab dengan uraian singkat dan bila perlu disertai gambar.

Diketahui nilai desimal huruf 'A' adalah 65 dan nilai desimal huruf 'Z' adalah 90.

1. Berdoalah, kemudian salinlah dan tandatangani pernyataan kejujuran sebagai berikut:

Saya, nama : ..... NIM : .....  
 mengerjakan ujian ini dengan jujur tanpa kecurangan. Tanda tangan : .....

2. {40%} Dalam kriptografi *block cipher*, dikenal mode ECB, CBC, CFB, dan OFB.

Gunakanlah 2 (dua) buah mode untuk mengenkripsi plainteks "INI" dengan ukuran blok(=unit)

8 (delapan) bit, kunci simetri 'K' dan proses enkripsi : XOR dilanjutkan 1 (satu) *circular-left-shift*.

Bila perlu, gunakan *initial vector* 'V'.

3. {40%} Dalam rangka pengiriman pesan rahasia, Alice dan Bob menyepakati penggunaan algoritma ElGamal dengan angka desimal 2 (dua) dan 97 (sembilan puluh tujuh). Alice memberi tahu Bob kunci publik hasil perhitungan atas kedua angka tersebut. Dengan informasi dari kunci publik Alice, Bob mengenkripsi pesan rahasianya menggunakan angka acak 7 (tujuh). Hasil enkripsi tersebut Bob kirimkan kepada Alice. Alice menerima cipherteks tersebut kemudian mendekripsinya menggunakan angka acak 5 (lima) sehingga mendapat isi pesan adalah "OK". Jelaskan proses pembangkitan kunci, enkripsi, dan dekripsi yang dilakukan oleh Alice dan Bob secara terstruktur !

4. {20%} Pada sebuah media jejaring sosial, seseorang menulis status sebagai berikut.

INI TINDAKAN NEKAD LHO. MAKAN SATE BELIBIS DITABURI LADA HALUS SEHINGGA KESAT LIDAHKU.

Status tersebut dicurigai mengandung pesan rahasia. Gunakanlah salah satu teknik Steganografi untuk mengekstraksi pesan yang tersembunyi !

Selamat mengerjakan dan semoga sukses.

# UJIAN TENGAH SEMESTER 2016/2017



**Ujian Tengah Semester Gasal 2016/2017  
Jurusan Ilmu Komputer/ Informatika  
FMIPA UNDIP Semarang**

---

Mata Kuliah : Kriptografi / Senin, 3 Oktober 2016  
Sifat : Buku Tertutup  
Waktu : 90 Menit

---

- Diketahui suatu ciphertext diperoleh dengan melakukan proses enkripsi terhadap suatu plainteks yang memanfaatkan algoritma Vigenere dengan kunci berupa nama dari suatu mata kuliah di Departemen Ilmu Komputer dan dilanjutkan dengan melakukan operasi transposisi dengan kunci = 5-3-2-4-1, apabila diketahui ciphertext yang dimaksud adalah

**MDHMWALLAEIJSOKZHYZHYMZDXMAMSAAEAL**

maka carilah Plaintextnya!

- Seorang kriptoanalisis mencoba menemukan plaintext dari suatu ciphertext sebagai berikut

**CYGPDLMHDKCUZQYWHOVMSYK**

Apabila dia menemukan bahwa metode yang digunakan untuk mengenkripsi plaintext yang dicari adalah dengan menggunakan Hill Cipher dengan matrik kunci

$$\text{Kunci} = \begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix}$$

maka bantulah kriptoanalisis tersebut untuk menemukan plaintext yang dimaksud!

# **UJIAN AKHIR SEMESTER 2016/2017**

## **UJIAN AKHIR SEMESTER**

PROGRAM STUDI : Teknik Informatika  
 MATA KULIAH : Kriptografi  
 HARI, TANGGAL : Senin, 05 Desember 2016  
 WAKTU : 60 menit  
 SIFAT : Buku Terbuka, boleh pakai kalkulator, android flight mode  
 PENGAMPU :  
     1. Helmie Arif Wibawa, S.Si, M.Cs  
     2. Nurdin Bahtiar, S.Si, M.T

**Jawablah setiap pertanyaan berikut dengan jelas dan singkat!**

1. Menggunakan metode OFB dan Key = **B**, enkripsi plainteks: **PARIT**  
 Catatan: Gunakan kode ASCII 8 bit. Output dalam bit. n = 4.
2. Jika S-Box di bawah ini digunakan untuk mensubstitusi string berikut, pesan apakah yang didapat?

S-Box:

0	75	83	72	85	70	77	86	82	78	73	79	89	76
1	81	65	86	79	83	74	66	71	90	88	68	82	70
2	85	80	76	87	80	78	67	74	81	65	89	73	88
3	72	84	69	66	68	87	90	71	84	67	69	75	77

String:

101010-010101-000011-101010-101111-110111-111001-101000-100100-000000-100101

--Selamat\_Mengerjakan--