

Ujian Tengah Semester **II4031 Kriptografi dan Koding**
Rabu, 27 Maret 2024
Waktu: 110 menit
Dosen: Rinaldi Munir

Berdoalah terlebih dahulu agar Anda berhasil dalam mengerjakan ujian ini!

1. Diketahui suatu cipherteks dengan *Caesar Cipher* seperti berikut "rfc ambc dmp rfc lcvr kecrgle gg gltglagzjc". Coba pecahkan cipherteks di atas dan sebutkan kuncinya.
2. Sebuah pesan rahasia (Bhs Indonesia) sepanjang 28 karakter dienkripsi dengan *product Cipher/super* enkripsi. Mula-mula pesan dienkripsi dengan *cipher* transposisi berbasis kolom seperti yang dijelaskan di dalam kuliah dengan kunci = ukuran kolom = 7. Selanjutnya hasilnya dienkripsi lagi dengan *Vigenere Cipher* dengan kalimat kunci = PANTAI SANUR (tidak termasuk spasi)
Cipherteks akhir yang dihasilkan adalah:

IENMOUCIYJBBOHNAVLYARPAWGNU

Dekripsilah cipherteks tersebut untuk mendapatkan kembali plaintekusnya!

3. Dekripsilah pesan berikut yang semula dienkripsi dengan *Playfair Cipher*:
QKNHKYEUSKOMTIKIFQUMITSTDTEFTV

Kunci yang digunakan adalah:

H	A	T	I	D
L	N	K	U	S
M	B	C	E	F
G	O	P	Q	R
V	W	X	Y	Z

4. (a) Diketahui sebuah gambar (*image*) berwarna berformat *bitmap* berukuran 800 x 600 pixel. Setiap *pixel* berukuran 3 *byte* (RGB). Jika dilakukan penyisipan pesan dengan metode LSB 2-bit (yaitu disisipkan pada 2 bit LSB pada setiap *byte*) ke dalam gambar tersebut, berapa ukuran maksimal pesan yang dapat disembunyikan di dalam gambar tersebut dalam satuan *byte*?
(b) Sebuah citra *grayscale* disisipi pesan dengan metode LSB 1-bit. Misalkan 8 buah *pixel* yang sudah disisipi bit pesan adalah sebagai berikut: 176, 177, 177, 178, 179, 179, 179, 180. Tentukan pesan yang diekstraksi dari keenam *pxiel* tersebut (dalam notasi bit dan heksadesimal)?
5. Diberikan sebuah cipherteks dalam notasi hexadecimal sebagai berikut: 4D29F53
(a) Ubah cipherteks dalam notasi biner
(b) Dekripsilah cipherteks tersebut dengan *stream cipher* sederhana (metode XOR). Kunci yang digunakan adalah F4 (dalam notasi *hexadecimal*). Tuliskan plainteks hasil dekripsinya dalam biner dan dalam heksadesimal
6. (a) Mengapa RC4 termasuk ke dalam algoritma kriptografi kunci-simetri? Jelaskan
(b) Proses apa yang dilakukan di dalam KSA?
(c) Apakah RC4 bisa digunakan untuk mengenkripsi file gambar dan video? Jelaskan.

7. Sebuah blok plainteks dalam matriks state sebagai berikut (dalam kode *hexadecimal*) akan dienkripsi dengan AES-128.

48	67	4d	d6
6c	1d	e3	5f
4e	9d	b1	58
ee	0d	38	e7

- (a) Tentukan isi matriks state setelah operasi SubBytes (lihat S-Box pada halaman lampiran)
- (b) Tentukan isi matriks state setelah operasi ShiftRows berdasarkan hasil dari (a)
- (c) Misalkan isi matriks state hasil operasi MixColumns berdasarkan hasil dari (b) adalah sbb:

$$\text{state} = \begin{bmatrix} 0f & 60 & 6f & 5e \\ d6 & 31 & c0 & b3 \\ da & 38 & 10 & 13 \\ a9 & bf & 6b & 01 \end{bmatrix} \text{ dan RoundKey} = \begin{bmatrix} ef & a8 & b6 & db \\ 44 & 52 & 71 & 0b \\ a5 & 5b & 25 & ad \\ 41 & 7f & 3b & 00 \end{bmatrix}$$

Tentukan isi matriks state setelah operasi AddRoundKey.

Nilai tiap soal:

- 1) 15; 2) 15 3) 15 4) 15 5) 15 6) 10 7) 15

LAMPIRAN

Vigenere Square

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

S-Box AES:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16