

Ujian Tengah Semester **II4021 Kriptografi dan Koding**
Kamis, 17 April 2025
Waktu: 110 menit
Dosen: Rinaldi

Berdoalah terlebih dahulu agar Anda berhasil dalam mengerjakan ujian ini!

1. Pesan “kejarlah daku kamu kutangkap” mula-mula dienkripsi dengan *cipher* transposisi (lebar kolom = 5), spasi dibuang, selanjutnya hasilnya dienkripsi dengan Vigenere Cipher dengan kata kunci = “MARKASCI PETE”, tentukan cipherteks akhirnya. (Tabel Vigenere terlampir) **(10)**

2. Dekripsilah pesan berikut yang semula dienkripsi dengan Playfair Cipher:

TDDVBUHEESIFCVCOIRGNFCRCOCCFIG

Kata kunci yang digunakan adalah KRIPTOGRAFIMANTAP

(10)

3. Sebuah pesan dienkripsi dengan *One-time pad* (OTP). Cipherteks yang dihasilkan adalah:

YAO LLUDDSQQUSIWHATEAMZKCPBNXCDEERX

Temukan **dua** buah kunci OTP yang menghasilkan plainteks berikut (spasi tidak termasuk):

(10)

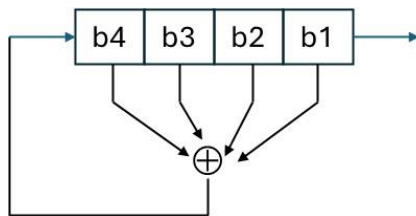
KAPAL SELAM MUSUH MENYUSUP DI SELAT BALI

4. Cipherteks berikut:

10101110101110001110001

didekripsi dengan *stream cipher* sederhana (metode XOR). Kunci yang digunakan adalah 11110000. Tuliskan plainteks hasil dekripsinya dalam biner dan dalam heksadesimal. **(5)**

5. Diberikan sebuah LFSR 4-bit. Fungsi umpan-balik adalah $b_4 = b_1 \oplus b_2 \oplus b_3 \oplus b_4$. Jika LFSR diinisialisasi dengan ‘1010’, tentukan bit-bit *keystream* yang dihasilkan sepanjang 15-bit pertama. **(10)**



6. (Nilai: 3 + 4 + 4 + 4)

(a) Berapakah ukuran blok (satuan bit), panjang kunci (satuan bit), dan jumlah putaran pada AES-256?

Sebuah blok plainteks dalam matriks *state* berikut (dalam kode Hex) akan dienkripsi dengan AES-128

aa	61	82	68
8f	dd	d2	32
5f	e3	4a	46
03	ef	d2	9a

(b) Tentukan isi matriks *state* setelah operasi *SubBytes* (lihat S-Box pada halaman lampiran)

(c) Tentukan isi matriks *state* setelah operasi *ShiftRows* berdasarkan hasil dari (a)

(d) Misalkan isi matriks *state* hasil operasi *MixColumns* berdasarkan hasil dari (b) adalah sbb:

state =

75	20	53	bb
ec	0b	c0	25
09	63	cf	d0
93	33	7c	dc

 dan RoundKey =

3d	47	1e	6d
80	16	23	7a
47	fe	7e	88
7d	3e	44	3b

Tentukan isi matriks state setelah operasi AddRoundKey.

7. (a) Diketahui sebuah gambar (image) berwarna berformat bitmap berukuran 800 x 600 pixel. Setiap pixel berukuran 3 byte (format RGB). Jika dilakukan penyisipan pesan dengan metode LSB 1-bit ke dalam gambar tersebut, berapa ukuran maksimal pesan yang dapat disembunyikan di dalam gambar tersebut dalam satuan byte? Hitung kembali jika pesan disisipkan pada 2-bit LSB. (5)
 (b) Sebuah citra grayscale disisipi pesan dengan metode LSB. 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 pixel tersebut (dalam notasi bit dan heksadesimal)? (5)
8. Diketahui kunci publik RSA milik Bob adalah $(e, n) = (26, 77)$. Alice mengenkripsi pesan dengan kunci public Bob tersebut. Misalkan Carol menyadap komunikasi Alice dan Bob dan berhasil memperoleh cipherteks dari Alice yaitu HBVO. Tentukan plainteks yang berhasil didekripsi oleh Carol dari cipherteks tersebut. Petunjuk: Ubah setiap huruf pada pesan menjadi angka dengan A = 0, B = 1, C = 2, D = 3, ..., Z = 25, lalu dekripsi masing-masing angka secara independen sebelum diubah kembali menjadi huruf yang bersesuaian. (10)
9. (a) Alice dan Bob akan berbagi kunci enkripsi simetri yang sama menggunakan algoritma Diffie-Hellman. Alice dan Bob menyepakati $g = 17$ dan $p = 37$. Alice memilih kunci privatnya $a = 7$ dan Bob memilih kunci privatnya $b = 9$. Tentukan kunci enkripsi yang dihasilkan oleh Alice dan Bob.
 (b) Jika kunci enkripsi simetri itu digunakan untuk mengenkripsi pesan dengan Caesar cipher, tentukan cipherteks yang dihasilkan untuk pesan "ADAAPADENGANMU". (10)
10. Sebuah pesan dalam biner '110011010101001001' dienkripsi dengan algoritma *knapsack* (Merkle-Hellman). Kunci privat adalah {3, 5, 15, 25, 54, 110}, parameter $n = 10$ dan $m = 39$. (12)
 - (a) Tentukan kunci publiknya
 - (b) Hitung cipherteks yang dihasilkan oleh proses enkripsi
 - (c) Hitung balikan modulo dari $n \pmod{m}$.
 - (d) Hitung plainteks yang dihasilkan dari proses dekripsi

Total Nilai = 102

=====

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