Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
==========

Ujian Tengah Semester **II4031 Kriptografi dan Koding**
Jumat, 11 Maret 2022
Waktu: 90 menit
Dosen: Rinaldi Munir

Berdoalah terlebih dahulu agar Anda berhasil dalam ujian ini!

1. Dekripsi cipherteks
   `AMTTT WAMYT LFDBC UNLDG CALXT`
   menggunakan *Vigenère cipher* dengan kuncinya adalah "PEOPLE". Plainteks dalam Bahasa Inggris. Susun kembali plainteks dalam kalimat Bahasa Inggris yang benar.

2. Sebuah pesan biner berikut:
   Plaintext: `1011100101101100 01`
   Kunci: `00110`

   Tentukan cipherteks yang dihasilkan jika pesan dienkripsi dengan *stream cipher*.

3. Misalkan pesan sudah dinyatakan dalam blok-blok plainteks sebagai berikut: P1, P2, P3, P4, dan P5. Blok cipherteks adalah C1, C2, C3, C4, dan C5.
   (a) Jika blok P2 diubah (misalnya karena rusak atau *corrupt*), maka blok cipherteks mana saja yang berubah jika dilakukan enkripsi dengan *block cipher* mode ECB, CBC, dan CFB?
   (b) Jika blok C2 diubah (misalnya karena rusak atau *corrupt*), maka maka blok plainteks mana saja yang berubah jika dilakukan dekripsi dengan *block cipher* mode ECB, CBC, dan CFB?

4. Diberikan sebuah blok plainteks dalam matriks 4 x 4 sebagai berikut (Gambar kiri). Notasi pesan dalam kode heksadesimal. Gambar kanan adalah S-box di dalam algoritma Rijndael.

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

	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

AES S-box

Tentukan isi blok plainteks setelah dilakukan berturut-turut transformasi *SubBytes* dan *ShiftRows*.

5. Sebuah citra berwarna 24-bit berukuran 500 x1000 *pixel*. Citra tersebut citra berwarna dengan komponen warna R, G, dan B (1 pixel terdiri dari R, G, dan B).
   (a) Berapa ukuran maksimum pesan yang dapat disembunyikan di dalam citra tersebut dengan metode LSB?
   (b) Misalkan diambil secuplik potongan gambar seukuran 3 pixel dengan nilai-nilai RGB dalam bit biner sebagai berikut:
   Pixel 1: 00101010, 01001101, 10000010
   Pixel 2: 01000011, 10001011, 10010000
   Pixel 3: 00110101, 00101000, 00101011

   Pesan yang akan disembunyikan adalah: 100110110.
   Tentukan nilai-nilai pixel (dalam biner dan dalam desimal) setelah disisipkan bit-bit pesan secara sekuensial dengan metode LSB

6. Sebuah pesan dienkripsi dengan algoritma RSA. Diktehui p = 11, q = 17, e = 107, dan d = 3. Jika cipherteks yang dihasilkan adalah c = 23, tentukan plainteksnya.