

UTS EL511 Kriptografi dan Aplikasinya – Remedial
 Senin, 25 November 2019
 Waktu: 2 jam

- Sebuah pesan rahasia “KIRIM SENJATA” dienkripsi dengan *Caesar Cipher* menggunakan $k = 13$.
 - Tuliskan ciphertekstnya
 - Jika pesan dienkripsi dua kali berturut-turut, apa hasilnya? (Nilai = 15)
- Sebuah pesan dienkripsi dengan *Playfair Cipher*. Kunci yang digunakan adalah “POLRES BANTUL”
 - Gambarkan bujursangkar 5×5 yang berisi huruf-huruf kunci
 - Enkripsilah pesan “MALAM MINGGU” dengan menggunakan kunci tersebut
 - Dekripsilah pesan “SN PF TN LD HL LR” dengan menggunakan kunci tersebut (Nilai = 20)
- Sebuah pesan biner “110100100111011” dienkripsi dengan algoritma XOR menggunakan kunci “1000”. Tentukan string biner hasil enkripsi. (Nilai = 10)
- Gambarkan diagram enkripsi dan dekripsi dengan menggunakan mode CBC. (Nilai = 10)
- Gambarkan diagram satu jaringan Feistel di dalam algoritma DES. (Nilai = 10)
- Diagram kotak-S di dalam algoritma AES adalah sebagai berikut:

	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

Sebuah blok pesan dalam matriks *state* adalah sebagai berikut:

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

- (a) Lakukan operasi *SubBytes* pada *state* tersebut dan tuliskan hasilnya dalam bentuk bujursangkar
- (b) Berdasarkan hasil dari *SubBytes* di atas, lakukan operasi *ShiftRows* dan tuliskan hasilnya dalam bentuk bujursangkar

(Nilai = 20)

7. Jelaskan istilah-istilah berikut:

- (a) Cipher
- (b) Kriptanalisis
- (c) Sebutkan empat layanan kriptografi

(Nilai = 15)