REPUBLIC OF INDONESIA DEFENSE UNIVERSITY
FACULTY OF SCIENCE AND DEFENSE TECHNOLOGY

MIDTERM EXAMS

Course	**: Military Cyrptography Technology**
Study Program	**: Cyber Defense Engineering**
Main Lecturer	**: Dr. Ir. Aulia Khamas Heikhmakhtiar, S.Kom., M.Eng**
Teaching Team	**: Dr. Ir. Rinaldi, M.T. Prof. Ir. Teddy Mantoro, Ph.D., SMIEEE**
Date	**: Tuesday, February 21, 2023 13.30 – 15.10 WIB**
Duration	**: 100 Minutes**
Nature of Exam	**: Open Book**

INSTRUCTIONS:

- **Read the exams rules and questions carefully.**
- **Answers are type in the following format: Arial (12), space 1.5., margin 3 cm for left-right-top-bottom.**
- **Your exam must be sent to the Google Drive with the following filename: absence number, study program, UAS, full name, subject and lecturer, Example: 02 - RPS - UAS- Hesty Friska – DRM - Major General Dr. Jonni Mahroza, S.IP., M.A., M.Sc., CIQnR, CIQaR**
- **No tolerance for cheating.**
- **Write the code (Study program_Cohort_Absence number), Example : RPS_Co1_02, in the top left in each answer sheet.**

QUESTIONS:

Bagian 1 Klasik Kriptografi

1. Apakah hasil dari Caesar chiper untuk pesan berikut ini jika key nya adalah a diubah menjadi u (sejauh 20 langkah). “i would like to see you tomorrow but i dont think i could”

2. Diketahui suatu sandi Caesar chiper seperti berikut “rfc ambc dmp rfc lcvr kccrgle gq gltglagzjc”. Coba pecahkan sandi di atas dan sebutkan key pada sandi tersebut!

3. Buatlah chiper text dengan metode OTP pada plaintext dan random key sebagai berikut.
   plaintext : jumlah kekuatan lawan adalah tiga ribu orang
   randkey : qwerty asdfghjk zxcvb yuioph fghj uytr mnbvc
   Chiper: ?

   Bagian 2 Steganografi

4. (a) Diketahui sebuah gambar (image) bewarna berukuran 800 x 600 pixel. Setap pixel berukuran 3 byte (format RGB). Jika dilakukan penyisipan pesan dengan metode LSB ke dalam gambar tersebut, berapa ukuran maksimal pesan (dalam satuan bit) yang dapat disembunyikan di dalam gambar tersebut?
   (b) Sebuah gambar sudah disisipi pesan sebanyak 8 bit dengan metode LSB. Pixel-pixel di dalam gambar adalah sebagai berikut:
   10001101, 10001101, 11001000, 10101010,
   10110101, 10101010, 11100110, 10010001
   Tuliskan hasil ekstraksi bi-bit pesan di dalam gambar tersebut, lalu nyatakan hasilnya dalam nilai desimal.

5. Planteks berikut:
   10101000101011101
   Akan dienkripsi dengan stream cipher sederhana (metode XOR). Kunci yang digunakan adalah 10011. Tuliskan cipherteks hasil enkripsinya.

6. Diketahui *S-box* di dalam AES dan sebuah plainteks (dinyatakan dalam matriks *state*).

	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

S-box

63	f2	30	fe
7c	6b	01	d7
77	6f	67	ab
7b	c5	2b	76

state

(a) Tuliskan *state* hasil operasi *SubBytes*
(b) Tuliskan *state* hasil operasi *ShiftRows* berdasarkan hasil dari (a)

7. (a) Gambarkan diagram mode CBC, baik untuk proses enkripsi maupun dekripsi
   (b) Gambarkan diagram mode *counter*, baik untuk enkripsi maupun dekripsi

ooooo <u>Good Luck</u> ooooo