

# UTS II4031 Kriptografi dan Koding - Sem 2 - 2022/2023

Ujian Tengah Semester  
Hari/Tanggal: Rabu 8 Maret 2023  
Waktu: 100 menit  
Sifat ujian: TUTUP BUKU

\* Required

1. Email \*

---

Data dan Pernyataan

Tuliskan nama, NIM, dan salin pernyataan

2. NIM \*

---

3. Nama \*

---

4. Tulis ulang pernyataan berikut: "Saya menyatakan bahwa saya mengerjakan UTS ini dengan sejujur-jujurnya, tanpa bantuan orang lain dan tanpa menggunakan cara yang tidak dibenarkan. Apabila di kemudian hari diketahui saya mengerjakan UTS ini dengan cara yang tidak jujur, saya bersedia mendapatkan konsekuensinya, yaitu mendapatkan nilai E pada mata kuliah II4031 Semester 2 Tahun 2022/2023. "
- 

#### A. SOAL PILIHAN BERGANDA

Pilihlah satu jawaban YANG

PALING BENAR. Soal UTS pilihan berganda terdiri dari total 20

pertanyaan. Setiap soal bernilai 3. Anda boleh menggunakan kalkulator, tetapi hanya

kakulator scientific di OS. Tidak diperkenankan menggunakan program

online yang ada di Internet. Setiap peserta ujian hanya boleh melakukan

submission/response sebanyak 1x saja menggunakan akun [@std.stei.itb.ac.id](mailto:std.stei.itb.ac.id)

5. Huruf plainteks yang sama tidak selalu dienkrpsi menjadi huruf cipherteks yang sama merupakan karakteristik cipher berikut:

*Mark only one oval.*

- Vigenere Cipher, Playfair Cipher, Affine Cipher
- Caesar Cipher, Vigenere Cipher, One-Time Pad
- Vigenere Cipher, Hill Cipher, Affine Cipher
- Vigenere Cipher, One-Time Pad, Hill Cipher
- Playfair Cipher, Vigenere Cipher, Affine Cipher, One-Time Pad
- One-Time Pad, Playfair Cipher, Affine Cipher
- Tidak ada jawaban yang benar

6. Layanan keamanan yang tidak disediakan oleh kriptografi adalah

*Mark only one oval.*

- Confidentiality, data integrity, availability
- Non-repudiation, control access, authentication
- Data integrity, denial of service, non repudiation
- Availability, control access, non-intrusion
- Authentication, data integrity, confidentiality, non repudiation, availability
- Tidak ada jawaban yang benar

7. Cipherteks OFINAQAHISIN didekripsi dengan Playfair Cipher menggunakan kunci NUSANTARA YANG INDAH, maka plainteks hasil dekripsi adalah

*Mark only one oval.*

- PERANAN NEGRI
- PERANKAN DIRI
- PEMDA SUMSEL
- PERATURAN BARU
- PERAN NEGARA
- PERANCIS BIRU
- Tidak ada jawaban yang benar

8. Hasil dekripsi ciphertexts NAEIOOBNEAA dengan Vigenere Cipher menggunakan kunci BATU adalah

*Mark only one oval.*

- MALING SABUN
- MALINO INDAH
- MALUKU UTARA
- MALAM MINGGU
- MALAS SEKALI
- Tidak ada jawaban yang benar

9. Plainteks HALO dienkripsi dengan Affine Cipher menggunakan  $m = 9$  dan  $b = 6$ , ciphertextsnya adalah:

*Mark only one oval.*

- ZOTS
- ZOME
- ZOTY
- ZOJK
- ZOLC
- Tidak ada jawaban yang benar

10. Sebuah mesin Enigma memiliki 4 buah rotor. Huruf-huruf plaintext hanya 8 buah, yaitu A, B, C, D, E, F, G, H. Jumlah kemungkinan substitusi huruf yang dapat dibuat oleh mesin Enigma tersebut adalah:

*Mark only one oval.*

- 4 x 8
- 4 x 8!
- 8 x 8 x 8 x 8
- 8!
- 8 x 8
- Tidak ada jawaban yang benar

11. Sebuah ciphertext "110100101011" adalah hasil enkripsi dengan algoritma XOR menggunakan kunci "1001". Tentukan plaintextnya dalam kode heksadesimal.

*Mark only one oval.*

- 8B3
- 4B0
- 5CF
- A5D
- 32F
- 4B2
- Tidak ada jawaban yang benar

12. Pernyataan manakah yang benar tentang RC4?

*Mark only one oval.*

- Pembangkitan kunci alir (keystream) terdapat di dalam subproses KSA
- Panjang kunci eksternal (dari user) harus sepanjang plainteks
- Pada dasarnya RC4 adalah sebuah keystream generator
- Kesalahan satu bit pada plainteks merambat pada seluruh bit cipherteks
- Keystream yang dibangkitkan oleh RC4 dapat tak terbatas banyaknya
- Tidak ada jawaban yang benar

13. Diketahui *S-box* di dalam AES dan sebuah plainteks (dinyatakan dalam matriks *state*). Baris-baris pada *state* adalah (dari paling atas) baris ke-0, ke-1, ke-2, dan ke-3. Nilai *state* pada baris ke-2 setelah dilakukan transformasi SubBytes adalah:

	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

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

*state*

*S-box*

Mark only one oval.

- F5, A8, 85, 62
- B6, 8A, 90, DC
- F3, 85, A7, 25
- E0, 52, 85, 26
- C5, A2, 81, 62
- Tidak ada jawaban yang benar

14. Perhatikan kembali 'state' pada soal sebelumnya. Jika dilakukan transformasi ShiftRows pada state tersebut, maka baris ketiga menjadi

*Mark only one oval.*

- tetap
- C5, 2B, 76, 7B
- 2B, 76, 7B, C5
- 76, 7B, C5, 2B
- Tidak ada jawaban yang benar

15. Misakan  $n$  = ukuran blok (bit),  $m$  = ukuran kunci (bit),  $r$  = jumlah putaran, maka nilai parameter yang benar untuk DES adalah

*Mark only one oval.*

- $n = 64, m = 64, r = 16$
- $n = 64, m = 64, r = 8$
- $n = 64, m = 56, r = 16$
- $n = 64, m = 56, r = 8$
- tidak ada jawaban yang benar



16. Sebuah citra grayscale disisipi pesan dengan metode LSB. Misalkan 8 buah pixel yang sudah disisipi bit pesan adalah sebagai berikut: 177, 177, 177, 178, 176, 179, 179, 180. Pesan yang diekstraksi dari keenam pixel tersebut (dalam notasi heksadesimal) adalah:

*Mark only one oval.*

- 5E
- F3
- B6
- A0
- E6
- AC
- Tidak ada jawaban yang benar

17. Sebuah citra berwarna berukuran 100 x 200 pixel, setiap pixel berukuran 3 byte. Kapasitas maksimal pesan yang dapat disembunyikan di dalam citra dengan metode LSB adalah (dalam satuan Kilobyte)

*Mark only one oval.*

- 7,1 KB
- 7,3 KB
- 7,5 KB
- 7,6 KB
- 7,7 KB
- tidak ada jawaban yang benar

18. Alice dan Bob akan berbagi kunci sesi  $K$  yang sama dengan algoritma Diffie-Hellman. Alice dan Bob menyepakati nilai  $g = 7$  dan  $p = 23$ . Alice memilih kunci privatnya  $a = 3$  dan Bob memilih kunci privatnya  $b = 6$ . Misalkan  $A$  dan  $B$  adalah masing-masing kunci publik Alice dan kunci publik Bob. Maka, nilai  $A$ ,  $B$ , dan  $K$  adalah

*Mark only one oval.*

- $A = 21, B = 4, K = 18$
- $A = 20, B = 17, K = 21$
- $A = 18, B = 17, K = 19$
- $A = 10, B = 13, K = 17$
- $A = 9, B = 12, K = 15$
- Tidak ada jawaban yang benar

19. Misalkan blok-blok plainteks adalah  $P_1, P_2, \dots, P_{10}$ , dan blok-blok cipherteks adalah  $C_1, C_2, \dots, C_{10}$ . Ukuran blok adalah 128bit. Sebuah cipher blok dioperasikan dalam mode counter. Jika blok  $C_2$  ada bit yang eror, maka hasil dekripsi yang eror adalah

*Mark only one oval.*

- $P_2$  dan  $P_3$
- $P_2, P_3, \dots, P_{10}$
- $P_2$  saja
- $P_1$  dan  $P_2$
- $P_1, P_2$ , dan  $P_3$
- Tidak ada jawaban yang benar

20. Algoritma kriptografi simetri apakah yang cocok diterapkan untuk enkripsi video yang ditransmisikan melalui saluran komunikasi, dalam hal ini kesalahan 1 bit dapat ditolerir tetapi penjalaran kesalahan tidak dibolehkan

*Mark only one oval.*

- A) Stream cipher
- B) Block cipher mode ECB
- C) Block cipher mode CFB
- D) Block cipher mode counter
- E) jawaban A dan B
- F) jawaban A, B, dan D
- G) Tidak ada yang benar

21. One-time pad tidak dapat dipecahkan karena

*Mark only one oval.*

- A) kunci hanya dipakai sekali
- B) kunci seluruhnya huruf-huruf semi-acak (pseudorandom)
- C) panjang kunci sepanjang pesan
- D) kunci tidak memiliki periode perulangan
- E) semua jawaban di atas benar
- F) hanya jawaban A, C, dan D yang benar
- G) Hanya jawaban A dan C yang benar

22. Parameter di dalam AES:

$n$  = ukuran blok (bit)

$m$  = panjang kunci (bit)

$r$  = jumlah putaran

Untuk AES-256, nilai  $n$ ,  $m$ , dan  $r$  adalah

*Mark only one oval.*

$n = 256, m = 256, r = 12$

$n = 128, m = 256, r = 12$

$n = 256, m = 256, r = 16$

$n = 128, m = 256, r = 14$

$n = 128, m = 256, r = 10$

$n = 256, m = 256, r =$

tidak ada jawaban yang benar

23. Parameter di dalam algoritma RSA:

$p, q$  : bilangan prima

$n = pq$

$\text{totient}(n) = (p-1)(q-1)$

$e$  : kunci enkripsi

$d$  : kunci dekripsi

Parameter apa saja yang rahasia?

*Mark only one oval.*

$p, q, e,$  dan  $\text{totient}(n)$

$p, q, n,$  dan  $\text{totient}(n)$

$p, q, d,$  dan  $n$

$p, q, d,$  dan  $\text{totient}(n)$

$p, q,$  dan  $d$  saja

tidak ada jawaban yang benar

24. Alice dan Bob berkirim pesan dengan menggunakan algoritma RSA. Misalkan:
- a dan A masing-masing kunci privat dan kunci publik Alice;
  - b dan B masing-masing kunci privat dan kunci publik Bob;
  - E : fungsi enkripsi
  - D : fungsi dekripsi
  - m : plainteks
  - c : cipherteks

Pernyataan mana yang benar pada enkripsi dan dekripsi pesan?

*Mark only one oval.*

- Alice:  $c = E(m)$  menggunakan A, Bob:  $m = D(c)$  menggunakan b
- Alice:  $c = E(m)$  menggunakan a, Bob:  $m = D(c)$  menggunakan b
- Alice:  $c = E(m)$  menggunakan B, Bob:  $m = D(c)$  menggunakan A
- Alice:  $c = E(m)$  menggunakan A, Bob:  $m = D(c)$  menggunakan B
- Alice:  $c = E(m)$  menggunakan B, Bob:  $m = D(c)$  menggunakan b
- Tidak ada jawaban yang benar

### Soal Essay

Jawablah soal essay pada kertas lembar jawaban (jangan di dalam google form)

25. 1. (Nilai= 12) Diberikan cipherteks hasil enkripsi pesan dengan One-Time Pad:  
NHYYSLKYBMNJA  
Temukan kunci one-time pad pertama yang menghasilkan plainteks MEET ME  
OUTSIDE, dan kunci one-time pad kedua yang menghasilkan plainteks HELP  
US SOMEONE
-

26. 2. (Nilai = 12)

(a) Apakah mode Counter membutuhkan fungsi dekripsi (D) dari block cipher?

Jelaskan jawaban anda dengan menggambar diagram mode Counter, baik untuk proses enkripsi dan dekripsi.

(b) Gambarkan diagram mode CBC untuk proses enkripsi dan dekripsi.

Menurutmu, apa bedanya mode CBC dengan mode counter?

---

27. 3. (Nilai = 6 + 5 + 5) Alice membangkitkan kunci publik dan kunci privatnya sebagai berikut. Alice memilih  $p = 13$  dan  $q = 17$ , lalu memilih kunci publiknya  $e = 5$ .

(a) Hitung kunci privat Alice

(b) Misalkan Bob mengirim pesan tiga huruf yaitu "SIP" kepada Alice. Hitung cipherteks yang dikirim kepada Alice (misalkan  $A = 00$ ,  $B = 01$ , ...,  $Z = 25$ )

(c) Hitung kembali plainteks hasil dekripsi oleh Alice

---

---

This content is neither created nor endorsed by Google.

Google Forms