UTS II4031 Kriptografi dan Koding - Sem 2 - 2021

* Required

1. Nama *

2. NIM *

3. 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 2020/2021. " *

4. Beberapa layanan yang disediakan oleh kriptografi adalah 4 points

Mark only one oval.

- Confidentiality, authentication, data integrity, availability
- Authentication, availability, non repudiation
- Data integrity, availability, confidentiality
- ✓ Confidentiality, authentication, data integrity
- Confidentiality, authentication, data integrity, availability, non-repudiation
- Confidentiality, authentication, availability, non-repudiation

5. Dua teknik dasar enkripsi di dalam kriptografi adalah teknik substitusi dan teknik transposisi. Mana diantara cipher di bawah ini yang BUKAN merupakan teknik transposisi. 4 points

Mark only one oval.

- [ ] Scrambling huruf-huruf di dalam pesan
- [ ] Menggeser sejumlah bit sejauh n bit ke kanan secara wrapping
- [x] Mengekpansi pesan dengan sejumlah bit tambahan
- [ ] Menyusun pesan secara vertikal per kolom dan membacanya secara horizontal
- [ ] Mempertukarkan bit ke-i dengan bit ke-(i+1)
- [ ] Tidak ada jawaban yang benar

6. Pesan "TERLALU" dienkripsi dengan Vigenere Cipher menggunkan kunci "KEY", maka cipherteks yang dihasilkan adalah (catatan: tidak perlu menggunakan Vigenere Square) 4 points

Mark only one oval.

- [x] DIPVEJE
- [ ] PDIJEVE
- [ ] IEPVDEJ
- [ ] VEJEPDI
- [ ] EIVJEPD
- [ ] Tidak ada jawaban yang benar

7. Pesan "HELLO TREE" dienkripsi dengan Playfair Cipher menggunakan kunci "KOTA BANDUNG". Jumlah digram yang terbentuk adalah 4 points

Mark only one oval.

- [ ] 4
- [ ] 5
- [x] 6
- [ ] 7
- [ ] 8
- [ ] Tidak ada jawaban yang benar

8. Lanjutan soal di atas. Hasil enkripsi pesan "HELLO TREE" dengan kunci "KOTA BANDUNG" menggunakan Playfair Cipher adalah: 4 points

Mark only one oval.

- [ ] IFHZFBAQHVVH
- [ ] IFBEQAHZVHVH
- [x] IFHZFBAQHVHV
- [ ] IFHZBFQAVHVH
- [ ] IFHZBFQAHVHV
- [ ] Tidak ada jawaban yang benar

9. Lanjutan soal di atas. Hasil dekripsi pesan "RK IB QV" dengan kunci "KOTA BANDUNG" menggunakan Playfair Cipher adalah 4 points

Mark only one oval.

- [ ] MALUKU
- [x] MALAM
- [ ] MUALIM
- [ ] MERAPI
- [ ] MAULUD
- [ ] Tidak ada jawaban yang benar

10. Pesan "KOTA" dienkripsi dengan Affine Cipher, m = 5, b = 10, n = 26. Cipherteksnya adalah: 4 points

Mark only one oval.

- [ ] MOKA
- [x] MGFO
- [ ] MTFB
- [ ] MRCX
- [ ] MYER
- [ ] Tidak ada jawaban yang benar

11. Cipher manakah yang memiliki karakteristik bahwa huruf plainteks yang sama tidak selalu dienkripsi menjadi huruf cipherteks yang sama? 4 points

Mark only one oval.

- A. Affine Cipher
- B. Vigenere Cipher
- C. Playfair cipher
- D. Hill cipher
- E. Semua jawaban di atas benar
- F. Hanya B, C, dan D yang benar
- G. Hanya A, B, dan C yang benar

12. Sebuah pesan biner “110100101011” dienkripsi dengan algoritma XOR menggunakan kunci “1000”. Tentukan string biner hasil enkripsi 4 points

Mark only one oval.

- 101001001000
- 101001011100
- 010110100011
- 001100110010
- 100110100011
- Tidak ada jawaban yang benar

13. One-time Pad tidak dapat dipecahkan karena 4 points

Mark only one oval.

- [ ] A. Panjang kunci sepanjang pesan
- [ ] B. Kunci adalah deretan karakater semi-acak
- [ ] C. Kunci digunakan hanya sekali
- [ ] D. Semua jawaban di atas benar
- [x] E. Hanya A dan C yang benar
- [ ] F. Tidak ada jawaban yang benar

14. Sebuah LFSR (Linear Feedback Shift Register) 4-bit dengan susunan bit-bit di dalam register adalah b3b2b1b0, fungsi umpan baliknya adalah b3 = f(b1, b2) = b1 XOR b2. Jika register diinisialisasi dengan bit 1001, maka 8 bit luaran (output) yang pertama adalah: 4 points

Mark only one oval.

- [x] 10010111
- [ ] 10010011
- [ ] 10010101
- [ ] 10011101
- [ ] 10011010
- [ ] Tidak ada jawaban yang benar

15. Pembangkitan keystream di dalam RC4 terdapat pada sub-proses 4 points

Mark only one oval.

- A. Keystream initialization algorithm
- B. Key scheduling algorithm
- ✓ C. Pseudo-random generation algorithm
- D. Semua jawaban benar
- ✓ E. B dan C saja
- F. Tidak ada jawaban yang benar

16. Sebuah pesan dibagi menjadi 8 buah blok, P1, P2, ..., P8. Misalkan pesan dienkripsi dengan sebuah block cipher dengan mode CBC. Hasil enkripsinya adalah blok-blok C1, C2, ..., C8. Misalkan pada proses dekripsi terjadi kesalahan bit pada C3. Maka hasil dekripsi yang salah adalah pada blok: 4 points

Mark only one oval.

- P3 saja
- P4 saja
- ✓ P3 dan P4 saja
- P3, P4, P5, P6, P7, P8
- P2 dan P3
- Semua jawaban salah

17. Misalkan L(i-1) dan R(i-1) adalah sub-blok pada putaran ke-(i-1), K(i) adalah kunci internal yang ke-i, maka persamaan sub-blok yang benar di dalam satu putaran DES adalah 4 points

Mark only one oval.

- [ ] R(i)= L(i − 1); L(i) = R(i −1) XOR f(L(i −1), K(i))
- [x] L(i)= R(i − 1); R(i) = L(i −1) XOR f(R(i −1), K(i))
- [ ] L(i)= R(i − 1); R(i) = R(i −1) XOR f(L(i −1), K(i))
- [ ] R(i)= L(i − 1); L(i) = L(i −1) XOR f(R(i −1), K(i))
- [ ] Tidak ada jawaban yang benar

18. Kesalahan satu bit pada blok cipherteks hanya mempengaruhi blok plainteks yang berkoresponden saja, merupakan karakteristik mode block cipher: 4 points

Mark only one oval.

- [ ] ECB
- [ ] OFB
- [ ] CFB
- [x] ECB dan OFB
- [ ] ECB dan CFB
- [ ] ECB, CFB, dan OFB
- [ ] Semua jawaban salah

19. Di dalam mode CBC, misalkan blok palinteks adalah P1 dan P2, blok cipherteks adalah C1 dan C2, dan initialization vector adalah IV. Maka peryataan yang benar adalah 4 points

Mark only one oval.

- A) C1 = IV XOR E(P1)
- B) C2 = E(C1 XOR P2)
- C) P1 = D(C1) XOR IV
- D) P2 = C1 XOR D(C2)
- E) Semua jawaban benar
- F) Hanya C dan D benar
- G) Jawaban B, C, dan D benar
- H) Semua jawaban salah

20. Mode counter memiliki karakteristik sebagai berikut: 4 points

Mark only one oval.

- A) Memerlukan initialization vector (IV)
- B) Melakukan chaining dengan blok-blok lain
- C) Pada proses dekripsi, nilai counter berkurang satu pada setiap dekripsi suatu blok
- D) Ukuran counter < ukuran blok
- E) semua jawaban benar
- F) semua jawaban salah

21. AES-128 memiliki karakteristik sebagai berikut: 4 points

Mark only one oval.

- A) Ukuran blok = 128 bit
- B) Panjang kunci bebas
- C) Jumlah putaran = 10 kali
- D) semua jawaban benar
- E) Hanya jawaban A dan C benar
- F) semua jawaban salah

22.

Mark only one oval.

- Option 1

23. AES memiliki satu kotak-S seperti gambar di bawah ini. Misalkan sebuah state adalah seperti pada gambar. Hasil transformasi SubBytes adalah 4 points

	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

19	A0	9A	E9
3D	F4	C6	F8
E3	E2	8D	48
BE	2B	2A	08

state

Mark only one oval.

24. Di dalam AES, ada empat transformasi, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Pernyataan yang benar tentang AES-128 (memiliki 10 putaran): 4 points

Mark only one oval.

- A. Jumlah transformasi MixColumns hanya 9 kali
- B. Jumlah transformasi AddRoundKey sebanyak 11 kali
- C. Jumlah transformasi ShiftRows sebanyak 10 kali
- D. Semua transformasi dilaksanakan masing-masing 10 kali
- E. Jawaban C dan D benar
- F. Hanya jawaban A dan C yang benar
- [x] G. Jawaban A, B, dan C benar

25. Sebuah S-box di dalam DES adalah seperti pada gambar. Misalkan input yang diterima adalah blok 6-bit berikut: 101100. Maka, output yang dihasilkan dari proses substitusi tersebut adalah: 4 points

S_2:

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Mark only one oval.

- 1010
- 0010
- 1011
- 1000
- 0100
- [x] Semua jawaban salah

26. Triple-DES dibuat untuk mengatasi kelemahan apa pada Double-DES? 4 points

Mark only one oval.

- ( ) Man-in-the-middle attack
- (✓) Meet-in-the-middle attack
- ( ) Intermediate attack
- ( ) Brute force attack
- ( ) Dictionary attack

27. Pesan apa saja yang bisa disembunyikan di dalam sebuah citra (image)? 4 points

Mark only one oval.

- ( ) Teks
- ( ) Citra
- ( ) Audio
- ( ) Video
- (✓) Semua jawaban di atas benar
- ( ) Hanya teks dan citra saja

28. Sebuah pesan berukuran 4 bit yaitu 1011 disembunyikan ke dalam empat buah pixel pada citra grayscale. Keempat pixel terebut bernilai 230, 228, 253, dan 240. Penyisipan dilakukan dengan metode LSB. Nilai-nilai pixel setelah penyisipan adalah 4 points

Mark only one oval.

- [ ] 231, 229, 254, 241
- [ ] 229, 227, 252, 239
- [x] 231, 228, 253, 241
- [ ] 231, 229, 252, 239
- [ ] 230, 229, 253, 240,
- [ ] Semua jawaban salah

29. Sebuah citra berwarna 24-bit (dengan komponen R, G, dan B) berukuran 100 x 100. Ukuran maksimum pesan yang dapat disembunyikan ke dalam citra tersebut adalah 4 points

Mark only one oval.

- [ ] 3000 bit
- [x] 30000 bit
- [ ] 1000 bit
- [ ] 10000 bit
- [ ] semua jawaban salah