UTS IF4020 Kriptografi - Sem 2 - 2022/2023

Ujian Tengah Semester
Hari/Tanggal: Selasa 7 Maret 2023
Waktu: 100 menit
Sifat ujian: TUTUP BUKU

* Required

1. Email *

Data dan Pernyataan

2. Nama *

3. NIM *

4. Tulis ulang pernyataan berikut:
"Saya menyatakan bahwa:
1. 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 IF4020 Semester 2 Tahun 2022/2023.
2. Tidak menyebarkan soal ujian kepada mahasiswa lain yang mengambil mata kuliah serupa. Apabila di kemudian hari diketahui saya menyebarkan soal ujian kepada mahasiswa lain, maka saya bersedia mendapatkan nilai E pada mata kuliah IF4020 Semester 2 Tahun 2022/2023 "

A. Soal Pilihan Berganda

Pilihlah satu jawaban YANG
PALING BENAR. Soal UTS pilihan berganda terdiri dari total 18 pertanyaan. Setiapsoal bernilai 3. Anda boleh menggunakan kalkultor, tetapi hanya
kakulator scientific di OS. Tidak diperkenankan menggunakan program online yang ada di Intenet. Setiap peserta ujian hanya boleh melakukan submission/response sebanyak 1x saja menggunakan akun @std.stei.itb.ac.id

5. Ruang kunci (key space) didefinisikan sebagai jumlah kemungkinan kunci yang dapat dibentuk untuk sebuah cipher. Di antara cipher berikut, cipher manakah yang memiliki ruang kunci paling besar? Alfabet yang dgunakan hanya A - Z.

Mark only one oval.

- [ ] Affine cipher
- [ ] Playfair cipher
- [x] Monoalphabetic cipher
- [ ] Vigenere cipher dengan panjang kunci = 10
- [ ] Enigma dengan 4 buah rotor
- [ ] Tidak ada yang benar

6. Huruf plainteks yang sama tidak selalu dienkripsi 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
- [x] 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

7. Cipherteks TRTA didekripsi dengan Playfair Cipher menggunakan kunci HAMPIR MALAM DI YOGYA, maka plainteks hasil dekripsi adalah

Mark only one oval.

- [ ] KOLI
- [ ] KODI
- [ ] KALI
- [x] KONI
- [ ] KOST
- [ ] Tidak ada jawaban yang benar

8. Misalkan kriptanalis menemukan sebuah pesan dienkripsi dengan Affine Cipher. Cipherteks 12 berkoresponden dengan plainteks 7, dan cipherteks 3 berkoreponden dengan plainteks 4.Tentukan nilai m dan b.

Mark only one oval.

- [ ] m = 3, b = 15
- [x] m = 3, b = 17
- [ ] m = 5, b = 15
- [ ] m = 5, b = 17
- [ ] m = 4, b = 12
- [ ] m = 4, b = 15
- [ ] tidak ada jawaban yang benar

9. Pernyataan manakah yang tidak benar tentang RC4?

Mark only one oval.

- [ ] Pembangkitan kunci alir (keystream) terdapat pada subproses PRGA
- [ ] Panjang kunci eksternal maksimal 256 byte
- [ ] Pada dasarnya RC4 adalah sebuah keystream generator
- [ ] Kesalahan satu bit pada plainteks hanya menghasilkan kesalahan pada cipherteks yang berkoresponden
- [x] Keystream yang dapat dibangkitkan oleh RC4 terbatas banyaknya
- [ ] Tidak ada yang salah pada semua pernyataan di atas

10. Sebuah LFSR (Linear Feedback Shift Register) 4-bit dengan susunan penomoran 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:

Mark only one oval.

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

11. Sebuah block cipher mengenkripsi blok pesan berukuran n bit. Block cipher tersebut dioperasikan masing-masing dengan mode ECB, CBC, CFB n-bit, OFB n-bit, dan Counter. Jika ada kesalahan satu bit pada blok cipherteks ke-i maka hanya mempengaruhi plainteks hasil dekripsi blok i saja. Karakteristik ini merupakan sifat dari mode operasi:

Mark only one oval.

- ECB, CFB
- ECB, CBC, CFB
- ECB, CFB, OFB, Counter
- ECB, CFB, Counter
- ECB dan Counter
- ECB saja
- Counter saja
- ✓ ECB, OFB, Counter
- Tidak ada jawaban yang benar

12. Mode operasi cipher blok yang dapat dibuat menjadi stream cipher adalah

Mark only one oval.

- A) Counter
- B) CFB 8-bit
- C) OFB 8-bit
- D) A, B, dan C benar
- ✓ E) B dan C benar
- F) A dan B benar
- Semua jawaban salah

13. Jaringan Feistel memiliki rumus berikut:
L(i) = R(i - 1)
R(i) = L(i - 1) XOR f(R(i - 1), K(i))

Jika diketahui L(1) dan R(1), maka R(0) dan L(0) pada proses dekripsi dapat diperoleh sebagai berikut:

Mark only one oval.

- ◯ R(0) = R(1); L(0) = L(1) XOR f(R(0), K(1))
- ◯ R(0) = R(1); L(0) = R(1) XOR f(R(0), K(1))
- ✓ R(0) = L(1); L(0) = R(1) XOR f(L(1), K(1))
- ◯ R(0) = L(1); L(0) = R(1) XOR f(R(1), K(1))
- ◯ R(0) = L(1); L(0) = L(1) XOR f(R(1), K(1))
- ◯ Tidak ada jawaban yang benar

14. Diketahui sebuah gambar (image) berwarna berformat bitmap 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 yang dapat disembunyikan di dalam gambar tersebut?

Mark only one oval.

- ◯ 180 KB
- ◯ 170,5 KB
- ◯ 177,8 KB
- ◯ 172,7 KB
- ✓ 175,8 KB
- ◯ Tidak ada jawaban yang benar

15. Efek confusion di dalam AES terdapat pada transformasi:

Mark only one oval.

- [ ] SubBytes
- [ ] ShiftRows
- [ ] MixColumn
- [ ] AddRoundKey
- [x] SubBytes dan AddRoundKey
- [ ] SubBytes dan MixColumn
- [ ] Tidak ada jawaban yang benar

16. 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-1 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

S-box

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

state

Mark only one oval.

- C6, 4E, CA, DF
- 10, 7F 7C, 0E
- 1B, F6, C3, EF
- 6C, E5, A8, 0F
- 8B, 61, 7D, 3b
- Tidak ada jawaban yang benar

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

Mark only one oval.

- 5E
- F3
- B6
- A0
- ✓ 6E
- AC
- Tidak ada jawaban yang benar

18. Sebuah pesan berukuran 6 bit yaitu 101101 disembunyikan ke dalam enam buah pixel pada citra grayscale. Keenam pixel tersebut bernilai 191, 187, 190, 189, 188, dan 200. Penyisipan dilakukan dengan metode LSB secara sekuensial. PSNR citra setelah dilakukan penyisipan pesan adalah sekitar (Catatan: rumus PSNR = 20 * log(255/rms). rms = sqrt(1/N * (Vi - V'i)^2). N = jumlah pixel, V = nilai pixel. Logaritma dalam basis 10)

Mark only one oval.

- 50
- ✓ 51
- 52
- 53
- 54
- Tidak ada jawaban yang benar

19. Diantara beberapa cipher blok berikut: GOST, RC5, RC6, Blowfish, Twofish, Serpent, MARS, dan AES, cipher mana sajakah yang tidak menggunakan jaringan Feistel?

Mark only one oval.

- ( ) Twofish, Serpent, AES
- ( ) Blowfish, MARS, Serpent
- ( ) RC5, RC6, Blowfish, Twofish
- ( ) AES, Twofish
- (✓) Serpent, MARS, AES
- ( ) GOST, RC5, RC6, Serpent
- ( ) Tidak ada jawaban yang benar

20. Alice dan Bob akan berbagi kunci sesi K yang sama dengan algoritma Diffie-Hellman. Alice dan Bob menyepakati nilai g = 7 dan p = 11. Alice memilih kunci privatnya a = 4 dan Bob memlih kunci privatnya b = 8. 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 = 9, B = 3, K = 5
- (✓) A = 3, B = 9, K = 5
- ( ) A = 9, B = 5, K = 8
- ( ) A = 5, B = 9, K = 8
- ( ) A = 5, B = 7, K = 6
- ( ) A = 7, B = 5, K = 6
- ( ) Tidak ada jawaban yang benar

21. Pernyataan yang SALAH tentang algoritma Diffie-Hellman

Mark only one oval.

- A) Digunakan untuk mengenkripsi kunci simetri
- B) Bilangan prima p rahasia
- C) Kunci publik Alice adalah A = g^a mod p (a adalah kunci privat Alice)
- D) Tidak dapat digunakan untuk mengenkripsi pesan
- Jawaban A dan D
- ✓ Jawaban A dan B
- Jawaban B dan D

22. Algoritma kriptografi kunc-publik yang mendasarkan keamanannya pada persoalan logaritma diskrit adalah

Mark only one oval.

- A) RSA
- B) ElGamal
- C) Diffie-Hellman
- D) ECC
- ✓ E) B dan C benar
- F) B dan D
- Tidak ada jawaban yang memenuhi

B. Soal Essay

Tuliskan jawaban soal essay ini pada kertas lembar jawaban

23. (Nilai = 10) Diketahui cipherteks hasil enkripsi dengan Caesar Cipher sebagai berikut:
USBSWCOXTKDKLOCYUWKVKW

Kunci (pergeseran huruf) tidak diketahui. Dekripsilah cipherteks tersebut. Pesan dalam Bahasa Indonesia.

KIRIM SENJATA BESOK MALAM

24. (Nilai = 11) Dekripsilah ciphertext berikut: KSWOOGVTRE
Cipherteks tersebut diperoleh dari enkripsi sebuah pesan dengan kombinasi dua buah cipher. Mula-mula pesan dienkripsi dengan Vigenere Cipher menggunakan kunci API, selanjutnya hasilnya dienkripsi lagi dengan Playfair Cipher dengan kunci WISUDA ITB GANESHA.

COKLAT MTDA atau COKLAT MUDA

25. (NIlai = 10) Diketahui kunci publik RSA adalah (e, n)= (107, 187). Misalkan diperoleh cipherteks c = 10. Dekripsilah cipherteks tersebut untuk mendapatkan plainteksnya.

p = 11, q = 17, totient(n) = 160, private key (d) = 3, plainteks (m) = 65

26. (Nilai = 15) Sebuah plainteks dalam biner: 1001010111000100. Misalkan sebuah block cipher melakukan enkripsi pesan dalam bentuk blok-blok, setiap blok berukuran 8-bit. Fungsi enkripsi E adalah sebagai berikut:
(i) pertukarkan bit ke-1 dengan bit ke-8, dan bit ke-4 dengan bit ke-5, bit-bit lainnya tetap.
(ii) selanjutnya XOR-kan hasil langkah (i) dengan kunci K yang panjangnya 8 bit.
Kunci K = 10101010

Pertanyaan:
a) Kodekan plainteks dalam notasi heksadesimal
b) Tentukan hasil enkripsi (dalam notasi heksadesimal) dengan block cipher tersebut dengan menggunakan mode CBC. Initial vector (IV) adalah 00000000
c) Ulangi kembali pertanyaan b di atas, tetapi menggunakan mode CFB 4-bit. Antrian (shift register) yang digunakan adalah dua elemen, setiap elemen panjangnya satu karakter heksadesimal (4-bit). Antrian diinisialisasi dengan IV = 00000000

(a) 95C4

(b) 2749

(c) 37C9
