UTS IF4020 Kriptografi - Sem 1 - 2021/2022

Semester 1 2021/2022

Pilihlah satu jawaban YANG PALING BENAR. Soal UTS terdiri dari total 25 pertanyaan, dengan waktu pengerjaan maksimal 100 menit. Boleh menggunakan kalkultor, tetapi hanya kakulator scientific di OS. Tidak diperkenankan menggunakan program onlne yang ada di Intenet. Setiap peserta ujian hanya boleh melakukan submission/response sebanyak 1x saja menggunakan akun @std.stei.itb.ac.id

	mail responden (null) dicatat saat formulir ini dil <mark>Wajib</mark>	kirimkan.
1.	Email *	
2.	Nama *	
3.	NIM *	
4.	Tulis ulang pernyataan berikut: "Saya mer ini dengan sejujur-jujurnya, tanpa bantua cara yang tidak dibenarkan. Apabila di ke UTS ini dengan cara yang tidak jujur, saya yaitu mendapatkan nilai E pada mata kuli *	n orang lain dan tanpa menggunakan mudian hari diketahui saya mengerjakan bersedia mendapatkan konsekuensinya

5.	Beberapa layanan yang TIDAK disediakan oleh kriptografi adalah
	Tandai satu oval saja.
	data integrity, availability
	data confidentiality, repudiation
	authentication, acces control, data integrity
	data confidentiality, authentication, data integrity
	acces control, availability
	denial of service, availability, acces control
	Tidak ada jawaban yang benar
6.	Dua teknik dasar enkripsi di dalam kriptografi adalah teknik substitusi dan teknik transposisi. Mana diantara cipher di bawah ini yang merupakan teknik transposisi.
	Tandai satu oval saja.
	A) Scrambling huruf-huruf di dalam pesan
	B) Merotasi sejumlah bit sejauh n bit ke kiri secara sirkuler
	C) Meng-XOR-kan bit plainteks dengan bit kunci
	D) Mempertukarkan bit ke-i dengan bit ke-(i+1)
	E) Semua jawaban benar
	F) Hanya A dan B yang benar
	G) A, B, dan D benar
	H) Tidak ada jawaban yang benar

7.	Diantara cipher klasik berikut: Vigenere Cipher, Affine Cipher, Hill Cipher, One- Time Pad, mana yang merupakan polyalphabetic cipher?
	Tandai satu oval saja.
	Vigenere Cipher
	Vigenere Cipher, One-Time Pad
	Vigenere Cipher, Hill Cipher
	Vigenere Cipher, Affine Cipher, Hill Cipher
	Vigenere Cipher, One-Time Pad, Hill Cipher
	Vigenere Cipher, Affine Cipher, One-Time Pad
8.	Dengan mengkodekan $A=0$, $B=1$, $C=2$,, $Z=25$, misalkan sebuah potongan cipherteks dari Vigenere Cipher adalah FOAC dan plainteks yang berkoresponden adalah MALU, maka tanpa bantuan Vigenere Square, kunci yang digunakan adalah
	Tandai satu oval saja.
	KONI
	TOMI
	ROTI
	ТОРІ
	ROTE
	◯ SOTO
	Tidak ada jawaban yang benar

9.	Pesan "HELLO TREE" dienkripsi dengan Playfair Cipher menggunakan kunci "KOTA BANDUNG". Jumlah digram yang terbentuk adalah
	Tandai satu oval saja.
	4
	5
	6
	8
	Tidak ada jawaban yang benar
10.	Lanjutan soal di atas. Hasil enkripsi pesan "HELLO TREE" dengan kunci "KOTA BANDUNG" menggunakan Playfair Cipher adalah:
	Tandai satu oval saja.
	IFHZFBAQHVVH
	IFBEQAHZVHVH
	IFHZFBAQHVHV
	IFHZBFQAVHVH
	IFHZBFQAHVHV
	Tidak ada jawaban yang benar

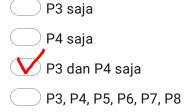
11.	Cipher manakah yang memiliki karakteristik bahwa huruf plainteks yang sama tidak selalu dienkripsi menjadi huruf cipherteks yang sama?
	Tandai satu oval saja.
	A. Affine Cipher
	B. Vigenere Cipher
	C. Playfair cipher
	D. Hill cipher
	E. Semua jawaban di atas benar
	F. Hanya B, C, dan D yang benar
	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 dalam kode heksadesimal.
	Tandai satu oval saja.
	4B2
	BC5
	√ 5A3
	F0A
	235
	BA3
	Semua jawaban salah

13.	One-time Pad tidak dapat dipecahkan karena
	Tandai satu oval saja.
	A. Panjang kunci sepanjang pesan
	B. Kunci adalah deretan karakater semi-acak
	C. Kunci digunakan hanya sekali
	D. Semua jawaban di atas benar
	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:
	Tandai satu oval saja.
	10010111
	10010011
	10010101
	10011101
	10011010

Tidak ada jawaban yang benar

15. 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:

Tandai satu oval saja.



P2 dan P3

Semua jawaban salah

16. Misalkan L(8) dan R(8) adalah sub-blok pada putaran ke-8, K(9) adalah kunci internal yang ke-9, maka persamaan L(9) dan R(9) yang benar di dalam satu putaran DES adalah

Tandai satu oval saja.

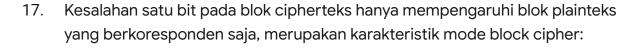
$$R(9) = L(8); L(9) = R(8) XOR f(L(8), K(9))$$

$$L(9) = R(8); R(9) = L(8) XOR f(R(8), K(9))$$

$$L(9) = R(8); R(9) = R(8) \text{ XOR } f(L(8), K(9))$$

$$R(9) = L(8); L(9) = L(8) XOR f(R(8), K(9))$$

____ Tidak ada jawaban yang benar



Tandai satu oval saja.



18. Di dalam mode CBC, misalkan blok plainteks adalah P1 dan P2, blok cipherteks adalah C1 dan C2, dan initialization vector adalah IV. Maka peryataan yang benar adalah

Tandai satu oval saja.

- 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

19.	Mode counter memiliki karakteristik sebagai berikut:
	Tandai satu oval saja.
	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
20.	AES-128 memiliki karakteristik sebagai berikut:
	Tandai satu oval saja.
	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

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

Tandai satu oval saja.

(Α. 、	Jumlah	transfor	masi M	lixColu	mns har	ıva 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

G. Jawaban A, B, dan C benar

22. Sebuah S-box di dalam DES adalah seperti pada gambar. Misalkan input yang diterima adalah blok 6-bit berikut: 111110. Maka, output yang dihasilkan dari proses substitusi tersebut adalah:

 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

Tandai satu oval saja.

() 1010

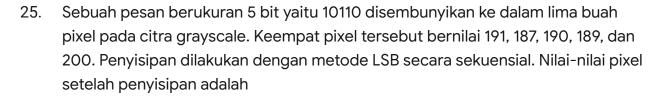
V 1111

1000

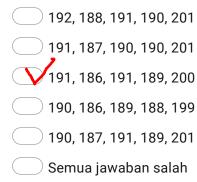
0100

Semua jawaban salah

23.	Triple-DES dibuat untuk mengatasi kelemahan apa pada Double-DES?
	Tandai satu oval saja.
	Man-in-the-middle attack
	Meet-in-the-middle attack
	Intermediate attack
	Brute force attack
	Dictionary attack
24.	Pesan apa saja yang bisa disembunyikan di dalam sebuah citra (image)?
24.	Pesan apa saja yang bisa disembunyikan di dalam sebuah citra (image)? Tandai satu oval saja.
24.	
24.	Tandai satu oval saja.
24.	Tandai satu oval saja. Kode program
24.	Tandai satu oval saja. Kode program Virus komputer
24.	Tandai satu oval saja. Kode program Virus komputer Binary data

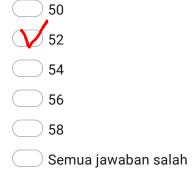


Tandai satu oval saja.



26. (lanjutan soal di atas) 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)

Tandai satu oval saja.



27. Sebuah citra berwarna 24-bit (dengan komponen R, G, dan B) berukuran 80 x 80 pixel. Ukuran maksimum pesan dalam satuan byte yang dapat disembunyikan ke dalam citra tersebut adalah

Tandai satu oval saja.

____ 800 byte

____ 1600 byte

2400 byte

6400 byte

Semua jawaban salah

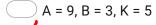
28. Pesan m = 32 akan dienkripsi dengan algoritma RSA. Nilai p = 5, q = 11. Kunci enkripsi e = 3. Nilai yang SALAH di bawah ini adalah

Tandai satu oval saja.

- A) n = 55
- B) toitent(n) = 40
- C) d = 28 (kunci dekripsi)
- D) c = 43 (cipherteks)
- E) jawaban C dan D
- 💮 F) Semua jawaban SALAH
- G) Semua jawaban benar, tidak ada yang salah

29. Alice dan Bob akan berbagi kunci sesi K yang sama dengan algoritma Diffie-Hellman. Alice dan Bob menyepakati nilai g = 7 dan n = 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

Tandai satu oval saja.



$$\triangle$$
 A = 3, B = 5, K = 9

Konten ini tidak dibuat atau didukung oleh Google.

Google Formulir