

Ujian Tengah Semester II4021 Kriptografi

Senin, 6 April 2026

Waktu: 120 menit

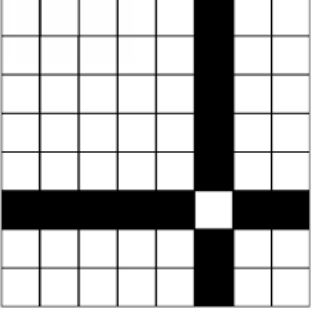
Dosen: Rinaldi M

Bagian A: Pilihan Ganda

Pilihlah satu jawaban yang benar, lalu **tuliskan jawaban** tersebut (huruf A, B, C, D, ..saja) pada lembar jawaban.
 Tiap soal bernilai 3 poin.

<p>1. Manakah layanan kriptografi yang menjelaskan bahwa pesan yang dikirim hanya bisa dibaca oleh penerima yang asli?</p> <p>A. Confidentiality B. Availability C. Authentication D. Data integrity E. Non repudiation</p>	<p>2. Diantara cipher klasik berikut: Vigenere Cipher, Affine Cipher, Hill Cipher, One-Time Pad, mana yang merupakan polyalphabetic cipher?</p> <p>A. Vigenere Cipher B. Vigenere Cipher, One-Time Pad C. Vigenere Cipher, Hill Cipher D. Vigenere Cipher, Affine Cipher, Hill Cipher E. Vigenere Cipher, One-Time Pad, Hill Cipher F. Vigenere Cipher, Affine Cipher, One-Time Pad</p>
<p>3. Hasil dekripsi dengan Vigenere Cipher untuk cipherteks MVGCSCSKD dengan kunci TEMPE adalah:</p> <p>A. TARUNAMAS B. TRUNOJOYO C. TRAUMAAKU D. TERBANGUN E. TERUSMAJU F. Tidak ada jawaban yang benar</p>	<p>4. Enkripsilah kalimat berikut THINK TWO GOOD THOUGHTS dengan menggunakan cipher transposisi, columnar transposition, dengan kata kunci MAYBE (spasi tidak dienkripsi):</p> <p>A. TTOU HWDG IOTH NGHT KOOS B. HWDG NGHT KOOS TTOU IOTH C. KOOS TTOU IOTH HWDG NGHT D. IOTH KOOS HWDG TTOU NGHT E. NGHT IOTH HWDG KOOS TTOU F. Tidak ada jawaban yang benar</p>
<p>5. Apa hasil dekripsi LTUQIDPO dengan Playfair Cipher, menggunakan kunci SECURITY (Catatan: X adalah karakter sisipan)?</p> <p>A. MITOLOGY B. MISSING C. MISSION D. MISSCALL E. MISSYOU F. Tidak ada jawaban yang benar</p>	<p>6. Ciphertext HZHSZBTILYIBUFP diperoleh dari Caesar Cipher dengan kunci yang tidak diketahui. Ciphertext tersebut dikriptanalisis dengan known-plaintext attack. Diketahui pasangan huruf plainteks S dan ciphetteks yang berkoresponden adalah Z. Maka, hasil kriptanalisis cipherteks tersebut adalah</p> <p>A. ASLI SUMBAR BARAT B. ASLI DARI VIETNAM C. ASAL SUMBER BUNYI D. ARAB SAUDI MENANG E. ATLIT SENAM INDAH F. Tidak ada jawaban yang benar</p>
<p>7. Sebuah pesan X terdiri dari 5 huruf: A, B, C, D, E. Peluang setiap huruf di dalam pesan adalah</p>	<p>8. String biner 1110101100011111 jika dikodekan ke dalam heksadesimal menjadi:</p> <p>A. C91F</p>

<p>$P(A) = \frac{1}{2}$; $P(B) = \frac{1}{4}$; $P(C) = \frac{1}{8}$; $P(D) = \frac{1}{16}$; $P(E) = \frac{1}{16}$. Entropi pesan X adalah:</p> <p>A. 1,525 bit B. 1,625 bit C. 1,725 bit D. 1,875 bit E. 1,925 bit F. Tidak ada yang jawaban benar</p>	<p>B. ED1F C. EA1F D. DB1F E. EB1F F. Tidak ada jawaban yang benar</p>
<p>9. Misalkan terdapat tiga buah blok plainteks, P1, P2, P3 dan P4 dan tiga buah blok cipherteks yang bersesuaian, C1, C2, C3 dan C4. Ketiga buah blok tersebut dienkripsi dengan sebuah block cipher dan mode operasi yang digunakan adalah CBC. Jika beberapa bit di dalam P2 eror (misalnya berubah dari 0 menjadi 1), maka cipherteks yang ikut mengalami kesalahan pada waktu enkripsi adalah:</p> <p>A. C1, C2, C3 dan C4 B. C2 saja C. C2 dan C3 D. C2, C3 dan C4 E. C4 saja F. Tidak ada jawaban yang benar</p>	<p>10. Misalkan terdapat tiga buah blok cipherteks, C1, C2, C3 dan C4 dan tiga buah blok plainteks yang bersesuaian, P1, P2, P3 dan P4. Ketiga buah blok tersebut didekripsi dengan sebuah block cipher dan mode operasi yang digunakan adalah OFB n-bit. Jika beberapa bit di dalam C2 eror (misalnya berubah dari 0 menjadi 1), maka plainteks yang ikut mengalami kesalahan pada waktu dekripsi adalah:</p> <p>A. P2 saja B. P2, P3 dan P4 C. P1, P2, P3 dan P4 D. P2 dan P3 E. P4 saja F. Tidak ada jawaban yang benar</p>
<p>11. Manakah dari pernyataan berikut yang paling tepat menggambarkan perbedaan utama antara enkripsi simetri dan asimetri (<i>public-key cryptography</i>)?</p> <p>A. Enkripsi asimetri umumnya lebih cepat daripada enkripsi simetri. B. Otentikasi pengirim pesan langsung diketahui pada enkripsi simetri C. Enkripsi simetri menggunakan dua kunci yang berbeda antara pengirim dan penerima pesan D. Enkripsi asimetri terutama digunakan untuk enkripsi data dalam volume yang besar. E. Tidak ada jawaban yang benar</p>	<p>12. Tiga buah pixel di dalam sebuah citra bernilai 125, 143, 150. Jika disisipkan pesan biner 101 ke dalam pixel-pixel tersebut dengan metode LSB, maka nilai-nilai pixel tersebut berubah menjadi:</p> <p>A. 126, 144, 151 B. 124, 142, 149 C. 125, 142, 151 D. 124, 144, 149 E. 125, 142, 149</p>
<p>13. 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 dengan metode 2-bit LSB adalah</p> <p>A. 3000 bit B. 30000 bit C. 6000 bit D. 60000 bit E. 10000 bit F. semua jawaban salah</p>	<p>14. AES-256 memiliki karakteristik sebagai berikut:</p> <p>A. Ukuran blok plainteks = 256 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</p>

<p>15. Sebuah <i>bitplane</i> pada metode BPCS steganography. Kompleksitas (α) <i>bitplane</i> tersebut adalah:</p>  <p>A. 28/112 B. 29/112 C. 30/112 D. 31/112 E. 32/112 F. Tidak ada jawaban yang benar</p>	<p>16. Kunci public RSA milik Bob adalah $(e, n) = (13, 33)$. Alice mengenkripsi pesan dan mengirim cipherteks $c = 26$ kepada Bob. Kunci privat Bob (d) dan plainteks hasil dekripsi (m) adalah:</p> <p>A. $d = 17, m = 5$ B. $d = 15, m = 8$ C. $d = 19, m = 10$ D. $d = 18, m = 7$ E. $d = 20, m = 11$ F. Tidak ada jawaban yang benar</p>
<p>17. Alice dan Bob akan berbagi kunci enkripsi simetri yang sama menggunakan algoritma Diffie-Hellman. Alice dan Bob menyepakati $g = 10$ dan $p = 541$. Alice memilih kunci privatnya $a = 5$ dan Bob memilih kunci privatnya $b = 7$. Tentukan kunci <i>shared key</i> yang dihasilkan oleh Alice dan Bob.</p> <p>A. 186 B. 201 C. 243 D. 193 E. 179 F. Tidak ada jawaban yang benar</p>	<p>18. Sebuah LFSR (<i>Linear Feedback Shift Register</i>) 4-bit dengan susunan bit di dalam register adalah $b_3b_2b_1b_0$, fungsi umpan baliknya adalah $b_3 = f(b_1, b_2) = b_1 \oplus b_2$. Jika register diinisialisasi dengan bit 1001, maka 8 bit luaran (output) yang pertama adalah:</p> <p>A. 10010111 B. 10010011 C. 10010101 D. 10011101 E. 10011010 F. Tidak ada jawaban yang benar</p>
<p>19. Pernyataan yang SALAH tentang algoritma Diffie-Hellman adalah:</p> <p>A. Digunakan untuk mengenkripsi kunci simetri B. Bilangan prima p rahasia C. Kunci publik Alice adalah $A = g^a \text{ mod } p$ (a adalah kunci privat Alice) D. Bukan algoritma untuk mengenkripsi pesan E. Jawaban A dan D F. Jawaban A dan B G. Jawaban B dan D</p>	<p>20. Algoritma kriptografi kunci-publik yang dapat digunakan untuk mengamankan transmisi kunci AES antara Alice dan Bob adalah</p> <p>A. RSA, ElGamal, Merkle-Hellman B. ElGamal, Diffie-Hellman C. Diffie-Hellman D. ElGamal dan Diffie-Hellman E. Merkle-Hellman, ElGamal, Diffie-Hellman F. RSA, ElGamal, Diffie-Hellman</p>

Bagian B: Soal Essay

Tuliskan jawaban Anda secara lengkap pada lembar jawaban. Setiap soal bernilai 10

1. Pecahkan *Affine Cipher* (cari nilai parameter m dan b) jika diketahui:

- huruf yang sering muncul di dalam cipherteks adalah 'X' ,
- huruf yang paling jarang muncul adalah 'U',
- trigram yang paling sering muncul adalah 'GEX'.

Semua pesan dalam Bahasa Inggris. Gunakan pengkodean karakter: A = 0, B = 1, C = 2, ..., Y = 24, Z = 25.

Verifikasi solusi Anda memenuhi semua kondisi yang disebutkan di atas dengan cara mendekripsi GEX.

2. Vigenere Cipher dimodifikasi sehingga semua plainteks, cipherteks, dan kuncinya adalah karakter heksadesimal (0..9, A..F).

a) Jika P_i adalah digit plainteks ke- i , C_i adalah digit cipherteks ke- i dan K_i adalah digit kunci, tuliskan persamaan enkripsi dan dekripsi Vigenere cipher tersebut:

$$E(P_i, K_i) = C_i = \underline{\hspace{10em}}$$

$$D(C_i, K_i) = P_i = \underline{\hspace{10em}}$$

b) Untuk plainteks $P = 3AE60A3$ dan kunci $K = 17E$, tentukan cipherteks C .

3. Tinjau sebuah *block cipher*, ukuran blok = ukuran kunci = 3 bit. Enkripsi setiap blok dengan kunci k dilakukan dengan persamaan berikut:

$$E_k(b_1b_2b_3) = (b_2b_1b_3) \oplus k$$

Tentukan hasil enkripsi pesan $m = 100100100$ dengan menggunakan kunci $k = 110$ dan mode operasi CBC, dengan IV = 111.

4. Alice akan mengenkripsi pesan biner 10101010 kepada Bob dengan algoritma Merkle-Hellman (*knapsack*). Bob memilih barisan *superincreasing* $w = (2,3,7,14,30,57,120,251)$, modulus $m = 491$ dan pengali = 41.

(a) Tentukan kunci publik dan kunci privat Bob

(b) Hitung cipherteks yang dikirim oleh Alice

(c) Bonus nilai (5): Tentukan hasil dekripsi cipherteks oleh Bob