Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

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.*

1. Manakah layanan kriptografi yang menjelaskan bahwa pesan yang dikirim hanya bisa dibaca oleh penerima yang asli? A. Confidentiality B. Availability C. Authentication D. Data integrity E. Non repudiation Jawaban: A	2. Diantara cipher klasik berikut: Vigenere Cipher, Affine Cipher, Hill Cipher, One-Time Pad, mana yang merupakan polyalphabetic cipher? 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 Jawaban: E atau B
3. Hasil dekripsi dengan Vigenere Cipher untuk cipherteks `MVGCSCSKD` dengan kunci `TEMPE` adalah: A. `TARUNAMAS` B. `TRUNOJOYO` C. `TRAUMAAKU` D. `TERBANGUN` E. `TERUSMAJU` F. Tidak ada jawaban yang benar Jawaban: B	4. Enkripsilah kalimat berikut `THINK TWO GOOD THOUGHTS` dengan menggunakan cipher transposisi, columnar transposistion, dengan kata kunci `MAYBE` (spasi tidak dienkripsi): 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 Jawaban: B
5. Apa hasil dekripsi `LTUQIDPO` dengan Playfair Cipher, menggunakan kunci `SECURITY` (Catatan: `X` adalah karakter sisipan)? A. `MITOLOGY` B. `MISSING` C. `MISSION` D. `MISSCALL` E. `MISSYOU` F. Tidak ada jawaban yang benar Jawaban: C	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 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 Jawaban: C

7. Sebuah pesan X terdiri dari 5 huruf: A, B, C, D, E. Peluang setiap huruf di dalam pesan adalah P(A) = ½; P(B) = ¼; P(C) = 1/8; P(D) = 1/16; P(E) = 1/16 . Entropi pesan X adalah:
   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

Jawaban: D

8. String biner 1110101100011111 jika dikodekan ke dalam heksadesimal menjadi:
   A. C91F
   B. ED1F
   C. EA1F
   D. DB1F
   E. EB1F
   F. Tidak ada jawaban yang benar

Jawaban: E

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:
   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

Jawaban: D

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:
   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

Jawaban: A

11. Manakah dari pernyataan berikut yang paling tepat menggambarkan perbedaan utama antara enkripsi simetri dan asimetri (*public-key cryptography*)?
   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 pengrim dan penerima pesan
   D. Enkripsi asimetri terutama digunakan untuk enkripsi data dalam volume yang besar.
   E. Tidak ada jawaban yang benar

Jawaban: B

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:
   A. 126, 144, 151
   B. 124, 142, 149
   C. 125, 142, 151
   D. 124, 144, 149
   E. 125, 142, 149

Jawaban: C

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
   A. 3000 bit

14. AES-256 memiliki karakteristik sebagai berikut:
   A. Ukuran blok plainteks = 256 bit
   B. Panjang kunci bebas
   C. Jumlah putaran = 10 kali
   D. semua jawaban benar

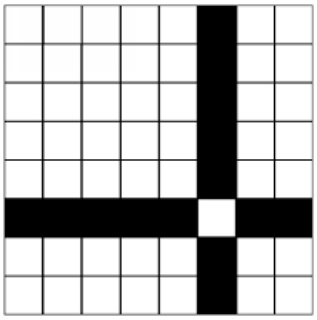
B. 30000 bit
C. 6000 bit
D. 60000 bit
E. 10000 bit
F. semua jawaban salah

Jawaban: D

E. Hanya jawaban A dan C benar
F. Semua jawaban salah

Jawaban: F

15. Sebuah *bitplane* pada metode BPCS steganography. Kompleksitas (α) *bitplane* tersebut adalah:



A. 28/112
B. 29/112
C. 30/112
D. 31/112
E. 32/112
F. Tidak ada jawaban yang benar

Jawaban: E

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:
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

Jawaban: A

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 *shared key* yang dihasilkan oleh Alice dan Bob.
A. 186
B. 201
C. 243
D. 193
E. 179
F. Tidak ada jawaban yang benar

Jawaban: D

18. Sebuah LFSR (*Linear Feedback Shift Register*) 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:
A. 10010111
B. 10010011
C. 10010101
D. 10011101
E. 10011010
F. Tidak ada jawaban yang benar

Jawaban: A

19. Pernyataan yang SALAH tentang algoritma Diffie-Hellman adalah:
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. Bukan algoritma untuk mengenkripsi pesan
E. Jawaban A dan D
F. Jawaban A dan B
G. Jawaban B dan D

Jawaban: F

20. Algoritma kriptografi kunci-publik yang dapat digunakan untuk mengamankan transmisi kunci AES antara Alice dan Bob adalah
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

Jawaban: A

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.

   Jawaban:
   Affine Cipher: $C \equiv (mP + b) \bmod 26$
   Dalam bahasa Inggris, huruf paling sering: **E** , huruf paling jarang: biasanya **Q** atau **Z**

   Dari soal: ciphertext paling sering = **X** , ciphertext paling jarang = **U**

   Dugaan: $E \rightarrow X \quad ; \; Z \rightarrow U$

   Kdekan $E = 4, X = 23, Z = 25, U = 20$

   Bentuk sistem persamaan:

$$\begin{array}{rl} 23 \equiv (4m + b) \pmod{26} & \\ 20 \equiv (25m + b) \pmod{26} & - \\ \hline 3 \equiv (4 - 25)m \pmod{26} & \\ 3 \equiv (-21)m \pmod{26} & \\ 3 \equiv 5m \pmod{26} & \rightarrow m = 11 \end{array}$$

   Sulihkan $m = 11$ ke dalam $23 \equiv (4\mathrm{m} + b) \pmod{26}$

$$\begin{aligned} 23 &\equiv (4(11) + b) \pmod{26} \\ 23 &\equiv (44 + b) \pmod{26} \\ b &\equiv -21 \pmod{26} \\ b &= 5 \end{aligned}$$

   Jadi, m = 11, b = 5

Verifikasi:

E → X : $(11 \cdot 4 + 5) \bmod 26 = 49 \pmod{26} = 23 = X$
Z → U : $(11 \cdot 25 + 5) \bmod 26 = 280 \pmod{26} = 0 = U$

Dalam bahasa Inggris, trigram paling sering = **THE**, dari soal trigram paling sering ciphertext = **GEX,** diduga THE → GEX
Kodekan: T = 19, H = 5, E = 4

T → ? $(11 \cdot 19 + 5) \bmod 26 = 214 \pmod{26} = 6 = G$ (cocok)

H → ? $(11 \cdot 7 + 5) \bmod 26 = 82 \pmod{26} = 4 = E$ (cocok)

E → ? $(11 \cdot 4 + 5)\ mod\ 26 = 49 \pmod{26} = 23 = X$ (cocok)

2. Vigenere Cipher dimodifikasi sehingga semua plainteks, cipherteks, dan kuncinya adalah karakter heksadesimal (0..9, A..F).
   a) Jika *Pi* adalah digit plainteks ke-*i*, *Ci* adalah digit cipherteks ke-*i* dan *Ki* adalah digit kunci, tuliskan persamaan enkripsi dan dekripsi Vigenere cipher tersebut:
      E(*Pi*,*Ki*) = C*i* = _____
      D(*Ci*,*Ki*) = *Pi* = _____
   b) Untuk plainteks P = 3AE60A3 dan kunci K = 17E, tentukan cipherteks C.

Jawaban:

a) *E*(*Pi*,*Ki*) = C*i* = (P1 + Ki) mod 16
D(*Ci*,*Ki*) = *Pi* = (Ci – Ki) mod 16

b) P = 3AE60A3
C = 17E17E1

(3 + 1) mod 16 = 4
(A + 7) mod 16 = 1
(E + E) mod 16 = C
(6 + 1) mod 16 = 7
(0 + 7) mod 16 = 7
(A + E) mod 17 = 8
(3 + 1) mod 16 = 4

Cipherteks: 41C7784

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.

Jawaban:

Enkripsi setiap blok dengan mode CBC: $C_i = E_k(P_i \oplus C_{i-1}), C_0 = IV$

Blok 1: $P_1 = 100, C_0 = 111$

$P_1 \oplus C_0 = 100 \oplus 111 = 011$

C_1 = E(011) = $101 \oplus 110 = 011$

Blok 2: $P_2 = 100, C_1 = 011$

$P_2 \oplus C_1 = 100 \oplus 011 = 111$

C_2 = E(111) = $111 \oplus 110 = 001$

Blok 3: $P_3 = 100, C_2 = 001$

$P_3 \oplus C_2 = 100 \oplus 001 = 101$

C_3 = E(101) = $011 \oplus 110 = 101$

Gabungkan semua blok: C = 011 001 101

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

Jawaban:

(a) Kunci privat dan kunci public:

Kunci privat = (2,3,7,14,30,57,120,251)

Menghitung kunci publik:

(2)(41) mod 491 = 82

(3)(41) mod 491 = 123

(7)(41) mod 491 = 287

(14)(41) mod 491 = 83

(30)(41) mod 491 = 248

(57)(41) mod 491 = 373

(120)(41) mod 491 = 10

(251)(41) mod 491 = 471

Kunci publik: (82, 123, 287, 83, 248, 373, 10, 471)

(b) Enkripsi

Pesan: $m = 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0$

$$C = 1(82) + 0(123) + 1(287) + 0(83) + 1(248) + 0(373) + 1(10) + 0(471)$$
$$= 82 + 287 + 248 + 10 = 627$$

Cipherteks: 627

(c) Dekripsi

◆ **Cari invers dari $r \bmod m$**

Cari r^{-1}sehingga: $41 \cdot r^{-1} \equiv 1 \bmod 491$
Hasil: $r^{-1} = 12$
Hitung: $C' = 627 \cdot 12 \bmod 491 = 159$

159 = 1 · 2 + 0 · 3 + 1 · 7 + 0 · 14 + 1 · 30 + 0 · 57 + 1 · 120 + 0 · 251

Palinteks = 10101010