Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
---

Ujian Tengah Semester **IF4020 Kriptografi**
Senin, 21 Oktober 2025
Waktu: 100 menit
Dosen: Dr. Ir. Rinaldi, M.T

---

*Berdoalah terlebih dahulu agar Anda berhasil dalam mengerjakan ujian ini!*

1. **(Nilai=10)** Diketahui suatu cipherteks dengan *Caesar Cipher* seperti berikut "rfc ambc dmp rfc lcvr kccrgle gq gltglagzjc". Coba pecahkan cipherteks di atas dan sebutkan kuncinya.

2. **(Nilai = 5)** Sebuah gambar berukuran 2 x 4 dienkripsi, sehingga nilai-nilai pixelnya (0 sampai 3) menjadi sebagai berikut:

| | | | |
|---|---|---|---|
| 1 | 0 | 0 | 3 |
| 2 | 3 | 1 | 3 |

   Hitung entropi gambar hasil enkripsi

3. **(Nilai = 10)** Sebuah pesan mula-mula dienkripsi dengan cipher transposisi (lebar kolom = 6), selanjutnya hasilnya dienkripsi lagi dengan Vigenere Cipher dengan kata kunci = "CIPETESELATAN", hasil akhirnya adalah cipherteks berikut:

   KUSRXWSERSBSZCBAENRSEXDISUWMGM

   Dekripsi Kembali cipherteks di atas menjadi plainteks (Tabel Vigenere terlampir)

4. **(Nilai = 10)** Diketahui sebuah gambar (image) berwarna berformat bitmap berukuran 2800 x 1600 pixel. Setiap pixel berukuran 3 byte (format RGB).
   (a) Jika dilakukan penyisipan pesan dengan metode LSB 1-bit ke dalam gambar tersebut, berapa ukuran maksimal pesan yang dapat disembunyikan di dalam gambar dalam satuan byte dan Kilobyte?
   (b) Apakah file berukuran 1500 KB dapat disisipkan ke dalam file gambar tersebut jika penyisipan pesan dilakukan pada 2-bit LSB?

5. **(Nilai = 10)** Pecahkan Affine Cipher jika diketahui bigram yang paling sering muncul di dalam cipherteks adalah JP. Lalu dekripsilah trigram 'IZW' (ini adalah trigram yang sering muncul di dalam teks Bahasa Inggris). Semua pesan dalam Bahasa Inggris. Gunakan pengkodean karakter: A = 0, B = 1, C = 2, …, Y = 24, Z = 25

6. **(Nilai = 5 + 5)** (a) Apa hasil operasi berikut dalam heksadesimal: 4BC91F $\oplus$ BA1DEC?
   (b) Apa hasil perkalian F2 $\cdot$ B9 dalam GF($2^8$) . Polinom irreduced polynom yang digunakan adalah $x^8 + x^4 + x^3 + 1$

7. **(Nilai = 15)** Sebuah plainteks (dalam heksadesimal), 4F51AC dienkripsi dengan sebuah block cipher. Ukuran blok yang dienkripsi adalah 8-bit dan kunci yang digunakan adalah 8-bit, yaitu B4. Fungsi enkripsi E yang digunakan adalah sebagai berikut:
   (i) Geser bit-bit di dalam pesan sejauh 2 bit ke kanan secara siklik
   (ii) XOR-kan hasil langkah (i) dengan kunci

   Tuliskan hasil enkripsi (dalam heksadesimal) untuk plainteks tersebut jika block cipher dioperasikan dengan mode:
   (a) ECB
   (b) CBC, IV = 00001111
   (c) Counter, dimulai dari counter awal 00000000

8. **(Nilai = 10)** Diketahui pasangan kunci publik dan kunci privat kepunyaan Tammy, Sonia, Farhan, dan Monalisa sebagai berikut:

**Tammy:**
Kunci public: (e, n) = (29,851)
Kunci privat: (d, n) = (1229,851)

**Sonia:**
Kunci public: (e, n) = (31,779)
Kunci privat: (d, n) = (1231,779)

**Farhan:**
Kunci public: (e, n) = (41,899)
Kunci privat: (d, n) = (881,899)

**Monalisa:**
Kunci public: (e, n) = (121,1591)
Kunci privat: (d, n) = (1537,1591)

Tammy mengirim pesan dan kunci enkripsi pesan (enkripsi menggunakan Vigenere Cipher) kepada Monalisa hybrid *cryptography* (RSA dan Vigenere Cipher). Pesan yang dienkripsi adalah SALAMSAYANGKUPADAMU dan kunci enkripsi adalah KOPIPAHIT. Cipherteks pesan dan cipherteks kunci dikirim bersamaan kepada Monalisa.
(a) Tuliskan cipherteks kunci dan cipherteks pesan yang dikirim oleh Tammy kepada Monalisa.
(b) Tuliskan hasil perhitungan dekripsi kunci dan dekripsi cipherteks yang diterima oleh Monalisa

9. **(Nilai = 10)** Diketahui kunci publik RSA Alice adalah (e, n) = (7, 187). Misalkan Eva memperoleh 3 buah cipherteks yang dikirim oleh Bob kepada Alice adalah 145, 108, 93. Eva mendekripsi ketiga buah cipherteks tersebut, lalu men-*decode* nya menjadi huruf-huruf plainteks (A = 0, B = 1, C = 2, …, Z = 25). Tuliskan plainteks yang didekripsi oleh Eva.

10. **(Nilai = 10)** Alice dan Bob akan berbagi kunci enkripsi simetri yang sama menggunakan algoritma Diffie-Hellman. Alice dan Bob menyepakati g = 10 dan p = 71. Alice memilih kunci privatnya a = 10 dan Bob memilih kunci privatnya b = 12. Tinjau dua kasus:
(a) Kasus 1: tidak terjadi *man-in-the-middle attack*. Tentukan kunci enkripsi simetri yang dihasilkan oleh Alice dan Bob
(b) Kasus 2: terjadi *man-in-the-middle attack*. Tiba-tiba Mallory mengintersepsi komunikasi dan melakukan serangan *man-in-the-middle attack* untuk mengetahui kunci enkripsi simetri Alice (K1) dan kunci enkripsi simetri Bob (K2). Mallory menggunakan kunci privatnya m = 15 di dalam serangan itu. Tentukan kunci enkripsi K1 dan K2 yang diperoleh oleh Mallory.

**LAMPIRAN** Vigenere Square

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |