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

Jawaban Ujian Tengah Semester **IF4020 Kriptografi**
Kamis, 28 Maret 2024
Waktu: 110 menit
Dosen: Rinaldi Munir

---

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

1. Sebuah pesan rahasia (Bhs Indonesia) sepanjang 35 karakter dienkripsi dengan *product Cipher*/super enkripsi. Mula-mula pesan dienkripsi dengan *cipher* transposisi berbasis kolom seperti yang dijelaskan di dalam kuliah dengan kunci = ukuran kolom = 7. Selanjutnya hasilnya dienkripsi lagi dengan *Playfair Cipher* dengan kalimat kunci = `SAMUDERA PASIFIK YANG LUAS BANGET` (tidak termasuk spasi)
Cipherteks akhir yang dihasilkan adalah:

`MYRSSYYIGKDSMSMRMYRGAIOADKRUGURUIMUM`

Dekripsilah cipherteks tersebut untuk mendapatkan kembali plainteksnya!

**Jawaban:**
Kunci Playfair:

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

Cipherteks: `MY RS SY YI GK DS MS MR MY RG AI OA DK RU GU RU IM UM`

Plainteks: `AN EA AK GR NL UD AD AP AN IY UR TD SL IA IX IA PU MA`

Selanjutnya didekripsi dengan cipher transposisi:
Panjang cipherteks = 35, Panjang kunci = 7, maka lebar kolom = 35/7 = 5
Buang huruf X

```
ANEAA
KGRNL
UDADA
PANIY
URTDS
LIAII
APUMA
```

Baca per kolom: `AKU PULANG DARI DARI PERANTAUAN DI DI MALAYSIA`

2. Sebuah pesan dienkripsi dengan *One-time pad* (OTP). Cipherteks yang dihasilkan adalah:

`IJUAGOTWRBJOCBWHCYWCAYJOCHTM`

Temukan dua buah kunci OTP yang berbeda sehingga dekripsi dengan OTP menghasilkan dua buah plainteks berbeda yang bermakna (dalam Bahasa Indonesia) sebagai berikut (tabel *Vigenere square* terlampir):
Kunci OTP ke-1 menghasilkan plainteks: `OMBAK BERGULUNG MENUJU KE ARAHKU`
Kunci OTP ke-2 menghasilkan plainteks: `SIAPA SURUH DATANG KE KALIMANTAN`

**Jawaban:**

Kunci 1: UXTAWNPFLHYUPVKDPENIQUJXCAJS

Kunci 2: QBULGWZFXUGOJBJBSUMCPQXOPOTZ

3. a) Diberikan 8 buah blok plainteks P1, P2, …, P6 dienkripsi dengan *Data Encryption Standard* (DES), hasilnya blok cipherteks C1, C2, …, C6. Mode operasi yang digunakan adalah ECB, CBC, CFB, OFB, dan Counter. Misalkan satu bit di dalam P2 dan P3 mengalami kesalahan bit. Tuliskan di dalam tabel berikut blok-blok cipherteks mana saja yang berubah akibat eror bit tersebut (tandai dengan √):

| Blok / Mode | C1 | C2 | C3 | C4 | C5 | C6 |
|---|---|---|---|---|---|---|
| ECB | | | | | | |
| CBC | | | | | | |
| OFB | | | | | | |
| CFB | | | | | | |
| Counter | | | | | | |

b) Diberikan 8 buah blok cipherteks C1, C2, …, C6 didekripsi dengan Data Encryption Standard (DES), hasilnya blok plainteks P1, P2, …, P6. Mode operasi yang digunakan adalah ECB, CBC, CFB, OFB, dan Counter. Misalkan satu bit di dalam C2 dan C3 mengalami kesalahan bit. Tuliskan di dalam tabel berikut blok-blok plainteks mana saja yang berubah akibat eror bit tersebut (tandai dengan √):

| Blok / Mode | P1 | P2 | P3 | P4 | P5 | P6 |
|---|---|---|---|---|---|---|
| ECB | | | | | | |
| CBC | | | | | | |
| OFB | | | | | | |
| CFB | | | | | | |
| Counter | | | | | | |

**Jawaban:**

a)

| Blok / Mode | C1 | C2 | C3 | C4 | C5 | C6 |
|---|---|---|---|---|---|---|
| ECB | | V | V | | | |
| CBC | | V | V | V | V | V |
| OFB | | V | V | | | |
| CFB | | V | V | V | V | V |
| Counter | | V | V | | | |

b)

| Blok / Mode | P1 | P2 | P3 | P4 | P5 | P6 |
|---|---|---|---|---|---|---|
| ECB | | V | V | | | |
| CBC | | V | V | V | | |
| OFB | | V | V | | | |
| CFB | | V | V | V | | |
| Counter | | V | V | | | |

4. Sebuah blok plainteks dalam matriks `state` sebagai berikut (dalam kode Hex) akan dienkripsi dengan AES-128

| | | | |
|---|---|---|---|
| 48 | 67 | 4d | d6 |
| 6c | 1d | e3 | 5f |
| 4e | 9d | b1 | 58 |
| ee | 0d | 38 | e7 |

(a) Tentukan isi matriks `state` setelah operasi `SubBytes` (lihat S-Box pada halaman lampiran)
(b) Tentukan isi matriks `state` setelah operasi `ShiftRows` berdasarkan hasil dari (a)
(c) Misalkan isi matriks `state` hasil operasi `MixColumns` berdasarkan hasil dari (b) adalah sbb:

`state` =

| | | | |
|---|---|---|---|
| 0f | 60 | 6f | 5e |
| d6 | 31 | c0 | b3 |
| da | 38 | 10 | 13 |
| a9 | bf | 6b | 01 |

dan `RoundKey` =

| | | | |
|---|---|---|---|
| ef | a8 | b6 | db |
| 44 | 52 | 71 | 0b |
| a5 | 5b | 25 | ad |
| 41 | 7f | 3b | 00 |

Tentukan isi matriks `state` setelah operasi `AddRoundKey`.

**Jawaban:**

**(a)**

| | | | |
|---|---|---|---|
| 52 | 85 | e3 | f6 |
| 50 | a4 | 11 | cf |
| 2f | 5e | c8 | 6a |
| 28 | d7 | 07 | 94 |

**(b)**

| | | | |
|---|---|---|---|
| 52 | 85 | e3 | f6 |
| a4 | 11 | cf | 50 |
| c8 | 6a | 2f | 5e |
| 94 | 28 | d7 | 07 |

**(c)**

| | | | |
|---|---|---|---|
| e0 | c8 | d9 | 85 |
| 92 | 63 | b1 | b8 |
| 7f | 63 | 35 | be |
| e8 | c0 | 50 | 01 |

5. Diketahui kunci publik RSA adalah (e, n) = (5, 221). Misalkan diperoleh cipherteks c = 153. Dekripsilah cipherteks tersebut untuk mendapatkan Kembali plainteksnya.

**Jawaban:**

$n = p \times q = 221 = 17 \times 13 \rightarrow p = 17, q = 13$

$\phi(n) = (p - 1)(q - 1) = (17 - 1)(13 - 1) = 192$

$ed \equiv 1 \pmod{\phi(n)} \rightarrow d = (1 + k\phi(n))/e = (1 + 192k)/5 \rightarrow$ untuk k = 2 diperoleh d = 77

$p = c^d \bmod n = 153^{77} \bmod 221 = 17$

6. Alice dan Bob akan berbagi kunci enkripsi simetri yang sama menggunakan algoritma Diffie-Hellman. Alice dan Bob menyepakati g = 11 dan p = 31. Alice memilih kunci privatnya a = 5 dan Bob memilih kunci privatnya b = 7. 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 = 8 di dalam serangan itu. Tentukan kunci enkripsi K1 dan K2 yang diperoleh oleh Mallory.

**Jawaban:**

$K1 = g^{am} \bmod p = (11)^{5 \times 8} \bmod 31 = 5$

$K2 = g^{bm} \bmod p = (11)^{7 \times 8} \bmod 31 = 7$

7. Sebuah pesan dalam biner '110011010101001001' dienkripsi dengan algoritma *knapsack* (Merkle-Hellman). Kunci privat adalah {3, 5, 15, 25, 54, 110}, parameter n = 10 dan m = 239.
(a) Tentukan kunci publiknya
(b) Hitung cipherteks yang dihasilkan oleh proses enkripsi

(c) Hitung balikan modulo dari n (mod m).
(d) Hitung plainteks yang dihasilkan dari proses dekripsi

**Jawaban:**

(a) 10 x 3 mod 239 = 30
10 x 5 mod 239 = 50
10 x 15 mod 239 = 150
10 x 25 mod 239 = 11
10 x 54 mod 239 = 62
10 x 110 mod 239 = 144

Kunci public = {30, 50, 150, 11, 62,144}

(b) P1 = 110011
C1 = 1 x 30 + 1 x 50 + 0 x 150 + 0 x 11 + 1 x 62 + 1 x 144 = 30 + 50 + 62 + 144 = 286

P2 = 010101
C2 = 0 x 30 + 1 x 50 + 0 x 150 + 1 x 11 + 0 x 62 + 1 x 144 = 50 + 11 + 144 = 205

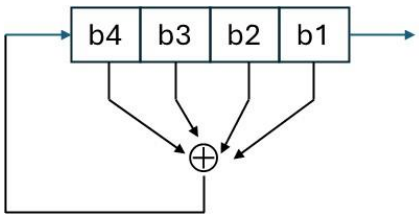
P2 = 001001
C2 = 0 x 30 + 0 x 50 + 1 x 150 + x 11 + 0 x 62 + 1 x 144 = 50 + 144 = 294

Cipherteks = (286, 205, 294)

(c) $n^{-1} \pmod m = 10^{-1} \pmod{239} = 24$

(d) 286 x 24 mod 239 = 172 = 3 + 5 + 54 + 110 → 110011
205 x 24 mod 239 = 140 = 5 + 25 + 110 → 010101
294 x 24 mod 239 = 125 = 15 + 110 → 001001

8. Diberikan sebuah LFSR 4-bit. Fungsi umpan-balik adalah b4 = b1 ⊕ b2 ⊕ b3 ⊕ b4. Jika LFSR diinisialisasi dengan '1010', tentukan bit-bit *keystream* yang dihasilkan sepanjang 15-bit pertama.




**Jawaban:**

| **Register** | **output** |
|---|---|
| 1010 | |
| 0101 | 0 |
| 0010 | 1 |
| 1001 | 0 |
| 0100 | 1 |
| 1010 | 0 |
| 0101 | 0 |

| | |
|---|---|
| 0010 | 1 |
| 1001 | 0 |
| 0100 | 1 |
| 1010 | 0 |
| 0101 | 0 |
| 0010 | 1 |
| 1001 | 0 |
| 0100 | 1 |
| 1010 | 0 |

Keystream: 010100101001010…

==========

**Nilai tiap soal:**

**1) 15 2) 10 3) 15 4) 15 5) 10 6) 10 7) 20 8) 10**

**Total nilai = 105**

## 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 |

S-Box AES:

| | 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 |