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

1. 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

1. 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 √):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| BlokMode | 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 √):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| BlokMode | P1 | P2 | P3 | P4 | P5 | P6 |
| ECB |  |  |  |  |  |  |
| CBC |  |  |  |  |  |  |
| OFB |  |  |  |  |  |  |
| CFB |  |  |  |  |  |  |
| Counter |  |  |  |  |  |  |

 **Jawaban:**

 a)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| BlokMode | 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)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| BlokMode | P1 | P2 | P3 | P4 | P5 | P6 |
| ECB |  | V | V |  |  |  |
| CBC |  | V | V | V |  |  |
| OFB |  | V | V |  |  |  |
| CFB |  | V | V | V |  |  |
| Counter |  | V | V |  |  |  |

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

 

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

state =  dan RoundKey = 

 Tentukan isi matriks state setelah operasi AddRoundKey.

 **Jawaban:**

1. **(b) (c)**

  

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

**Jawaban:**

 n = p x q = 221 = 17 x 13 🡪 p = 17, q = 13

 φ(n) = (p – 1)(q – 1) = (17 – 1)(13 – 1) = 192

 ed ≡ 1 (mod φ(n) ) 🡪 d = (1 + kφ(n))/e = (1 + 192k)/5 🡪 untuk k = 2 diperoleh d = 77

 p = cd mod n = 15377 mod 221 = 17

1. 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 = gam mod p = (11)5 x 8 mod 31 = 5

K2 = gbm mod p = (11)7 x 8 mod 31 = 7

1. 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.
2. Tentukan kunci publiknya
3. Hitung cipherteks yang dihasilkan oleh proses enkripsi
4. Hitung balikan modulo dari n (mod m).
5. Hitung plainteks yang dihasilkan dari proses dekripsi

**Jawaban:**

1. 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}

1. 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)

1. n–1 (mod m) = 10–1 (mod 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

1. 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



S-Box AES:

