Matkul: Kripto

INSTITUT TEKNOLOGI DEL

UJIAN TENGAH SEMESTER

Semester V T.A. 2023/2024

Hari, Tanggal	:	Kamis, 19 Oktober 2023
Kode – Nama Mata Kuliah	:	11S3105 – Kriptografi dan Keamanan Informasi
Tipe Ujian	:	Teori
Durasi Pengerjaan	:	110 Menit
Pengampu	:	JHS, IUS

PETUNJUK

Sebelum mengerjakan soal UTS, bacalah petunjuk pengerjaan berikut ini:

1. Terdapat 2 tipe soal, Multiple Choice (MC) 12 soal dan Essay 4 soal dengan total 16 soal dan100 point.
2. Jawaban untuk **tipe soal MC harus dituliskan secara berurutan**, sedangkan **tipe soal Essay dapat dituliskan tidak berurutan**, tetapi tuliskan penomoran dengan jelas.
3. Soal ujian dapat dicoret-coret jika anda membutuhkan tempat untuk jawaban sementara.
4. Jawaban ditulis menggunakan pulpen.
5. Selama ujian mahasiswa hanya diperbolehkan menggunakan kalkulator sebagai alat bantu hitung.
6. Ujian bersifat tertutup (*closed book*). Peserta tidak diperkenankan membuka sumber lainnya selain soal yang diberikan serta bekerja sama dengan orang lain. Pelanggaran akan mengakibatkan hukuman sesuai aturan akademik yang berlaku di IT Del dan nilai UTS 0.

BERKAS SOAL UJIAN DIKUMPULKAN KEMBALI

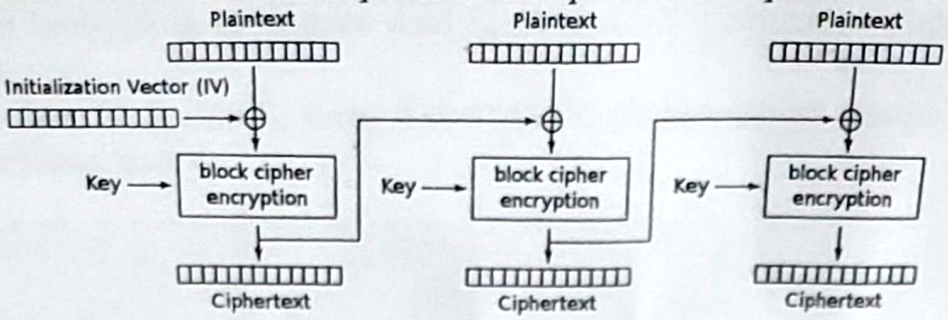
18

BAGIAN A. MULTIPLE CHOICE (30 Poin)

Pilih salah satu jawaban yang benar.

1. (2 poin) Di bawah ini manakah yang termasuk dalam jenis serangan aktif (*active attack type*)?
   a. Daniel of Service, Reply, dan Masquerade
   b. Daniel of Service, Release of message contents, dan Masquerade
   c. Release of message contents, Traffic analysis, dan Masquerade
   d. Modification of messages, Release of message contents, dan Daniel of Service
   e. Modification of messages, Traffic analysis, dan Daniel of Service
2. (2 poin) Pesan yang telah disandikan sehingga tidak bermakna lagi disebut:
   a. *Plaintext*
   b. *Ciphertext*
   c. *Encryption*
   d. *Decryption*
   e. *Cryptography*
3. (5 poin) Apakah *ciphertext* dari plaintext "SUN" yang menggunakan teknik enkripsi Caesar *cipher* dengan kunci 4?
   a. UNS
   b. VXQ
   c. WYR
   d. VYR
   e. WXR
4. (2 poin) *Interruption* adalah serangan terhadap aspek:
   a. *Availability*
   b. *Confidentiality*
   c. *Integrity*
   d. *Authenticity*
   e. *Non-Repudiation*
5. (2 poin) *Interception* adalah serangan terhadap aspek:
   a. *Availability*
   b. *Confidentiality*
   c. *Integrity*
   d. *Authenticity*
   e. *Non-Repudiation*
6. (2 poin) *Cipher* yang mengenkripsi pasangan huruf (*bigram*) adalah:
   a. Caesar *cipher*
   b. Vigenere *cipher*
   c. Rail Fence *cipher*
   d. Playfair *cipher*
   e. Tidak ada pilihan jawaban yang benar
7. (2 poin) Mengenkripsi *plaintext* menjadi chipertext setiap bit per bit dengan bit-bit kunci disebut:
   a. Caesar *cipher*
   b. Vigenere *cipher*
   c. *Advanced Encryption Standard* (AES)
   d. *Stream cipher*
   e. *Block cipher*

8. (2 poin) Gambar di bawah ini merupakan mode operasi blok *cipher*:



a. *Electronic Code Book (ECB)*
b. *Cipher Block Chaining (CBC)*
c. *Cipher Feedback (CFB)*
d. *Output Feedback (OFB)*
e. *Counter Mode*

9. (2 poin) Setiap blok *plaintext* P_i dienkripsi secara individual dan *independent* dari blok lainnya menjadi blok *ciphertext* C_i disebut:
a. *Electronic Code Book (ECB)*
b. *Cipher Block Chaining (CBC)*
c. *Cipher Feedback (CFB)*
d. *Output Feedback (OFB)*
e. *Counter Mode*

10. (2 poin) Di dalam mode operasi *Cipher Block Chaining* (CBC), blok *plaintext* saat ini akan ditambahkan (XOR) dengan:
a. Blok *ciphertext* sebelumnya
b. Blok *ciphertext* selanjutnya
c. Blok *plaintext* sebelumnya
d. Blok *plaintext* selanjutnya
e. Tidak ada pilihan jawaban yang benar

11. (2 poin) Di bawah ini mode operasi blok *cipher* yang memperlakukan *cipher* blok sama seperti *stream cipher* adalah:
a. *Electronic Code Book (ECB)*
b. *Cipher Block Chaining (CBC)*
c. *Cipher Feedback (CFB)*
d. *Counter Mode*
e. Tidak ada pilihan jawaban yang benar

12. (5 poin) Di berikan sebuah *plaintext* 1010 0010, key 1011, serta fungsi enkripsi XOR kan blok *plaintext* P_i dengan K, kemudian geser bit-bit dari $P_i + K$ dua posisi ke kiri. Hasil *ciphertext* dari *plaintext* tersebut menggunakan mode operasi ECB adalah:
a. 1010 1000
b. 0001 1001
c. 0010 0011
d. 0100 0110
e. 1010 0010

1010 0010
1011 1011
0001 1001
0100 0110

BAGIAN B. ESSAY (70 Poin)

Tuliskan jawaban yang lengkap di lembar jawaban yang disediakan

1. **(20 Poin)** Tentukan bit dari kata **CRYPTO**. Hasil bit dari kata tersebut adalah blok A sepanjang 48 bit hasil ekspansi $E(R_{i-1})\oplus K_i$ dengan menggunakan algoritma DES.

18+42 = (60) 42

NIM : 11521001
NAME : Rafi Virgan Gunawan
SUBJECT : Kriptografi
ACKNOWLEDGEMENT & SIGNATURE : I AGREE TO SIT THIS EXAM IN AN HONEST AND FAIR MANNER

Essay :

1). Tentukan bit dari CRYPTO :

C = 43 = 0100 0011 ✓
R = 52 = 0101 0010 ✓
Y = 59 = 0101 1001 ✓
P = 50 = 0101 0000 ✓
T = 54 = 0101 0100 ✓
O = 4F = 0100 1111 ✓

17

Sehingga didapat :

010000 110101 001001 011001 010100 000101 010001 001111
S1 S2 S3 S4 S5 S6 S7 S8.

S_1 = 010000
S_3 = 001001
S_5 = 010100

=> 010000 (0, 8.) baris : 0, kolom : 8 → jadi $S_1 = 3$ ✓ Bit ?

=> 001001 (1, 4) baris : 01, kolom : 4 → jadi $S_3 = 3$ ✓ Bit ?

=> S_5 = 010100 (10, 0) baris : 0, kolom : 10 → jadi $S_5 = 3$ ✓ Bit ?

gunakan fermats/euler : $3^{302} \bmod 11$ & $3^{154} \bmod 45$

a) $3^{302} \bmod 11$ ⟨11 → bil.prima⟩

dengan fermat :

$3^{10} = 1 \pmod{11}$

$3^{302} = 3^{10 \cdot 30 + 2} \pmod{11}$

$= 1^{30} \cdot 3^2 \pmod{11}$

$= 9$ //

b). 45 ≠ bil.prima → euler's :

$\phi(45) = 3^2 \times 5$

$= (3^2 - 3^1) \times (5 - 1)$

$= 6 \times 4 = 24$. ✓

15

jadi :

$3^{23} = x \pmod{24}$

$3^{154} = 3^{23 \cdot 8 + 10} \pmod{24}$

$= x(3^{10} \bmod 24)$

$3^{154} = 3^{23 \cdot 8 + 10} \pmod{24}$ ✓

$= 3^{10} \pmod{24} = 9$

(3). dik:

EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D6

dit: input bytes kol-4, untuk baris -2 & -3.

Penyelesaian:

$S'_{0,3} = (S_{0,3})(02) + (S_{1,3})(03) + (S_{2,3})(01) + (S_{3,3})(01)$

-> $S_{0,3} = 7B = (0111\ 1011)\ (02)$

-> $S_{1,3} = 7D = (0111\ 1101)\ (03)$

-> $S_{2,3} = 26 = (0010\ 0110)\ (01)$

-> $S_{3,3} = C3 = (1100\ 0011)\ (01)$.

$S'_{0,3} = 0111\ 1011 \oplus 0000\ 0010$ (+) $= 0111\ 1001$

$0111\ 1101 \oplus 0000\ 0100$ (+) $= 0111\ 1001$

$0010\ 0110 + 1100\ 0011$

(3).

EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D6

shiftrows =D

EB	59	8B	1B
2E	A1	C3	40
13	42	F2	38
E7	D6	1E	84

2

dik : $p(x) = x^8 + x^4 + x^3 + x + 1$.

$S_{0,3} = (S_{0,3})(02) + (S_{1,3})(03) + (S_{2,3})(01) + (S_{3,3})(01)$

=D -> $S_{0,3} = 7B = (0111\ 1011)\ (02) = (1000\ 0010)$

-> $S_{0,3} = 7D = (0111\ 1101)\ (03) = (0111\ 1110)$

-> $S_{2,3} = 26 = (0010\ 0110)\ (01) = (0010\ 0110)$

-> $S_{3,3} = C3 = (1100\ 0011)\ (01) = (1100\ 0011)$ (+)

$0100\ 1\ 101$

-> $S_{0,3} = 0111\ 1011$

10 (+)

$0111\ 1001$ =D $x^6+x^5+x^4+x^3+1$.

$= 79$. $p(x) = x^8+x^4+x^3+x+1$

$x^6+x^5+x^4+x^3+1 \;/\; x^8+x^4+x^3+x+1 = 1$

$x^8+x^4+x^3+x+1 = 01000111$

$x^6+x^5+x^2+x^2+1 = 00111101$ (+)

10000010

X

yadi $S'_{0,3} = 0100\ 1101$.

$S'_{2,3} = (s_{0,3})(02) + (s_{1,3})(03) + (s_{2,3})(01) + (s_{3,3})(01)$

→ $s_{0,3} = 7B = (0111\ 1011)(02) =$ ~~(1000 0010)~~ $(0111\ 1001)$

$s_{1,3} = 7D = (0111\ 1101)(03) = (0111\ 1110)$

$s_{2,3} = 26 = (0010\ 0110)(01)\ (1001\ 1001)$ ④

$s_{3,3} = C3 = (1100\ 0011)(01) = (1100\ 0011)$ ①

$(0101\ 1100)$

$x^5+x^3+x^2$ | $x^8+x^4+x^3+x+1$ = 1000 1121.

$x^5+x^3+x^2$ = 0001 0110 ④

1001 1001

jadi $S'_{2,3} = 0101\ 1100$

---

⑤. Tentukan Multiplication & Multiplication Inverse! GF(4)!

$P(x) = x^2+x+1$

→ Multiplication:

	(0) 00	(1) 01	(x) 10	(x+1) 11
(0) 00	0	0	0	0
(1) 01	0	1 ✓	x ✓	x+1 ✓
(x) 10	0	x ✓	x^2 ✗	1 ✓
(x+1) 11	0	x+1 ✓	1 ✓	x ✓

x^2+x+1 | x^2+x+1 = 0 0 0 1 1 0

x^2+x+1 = 0 1 1 1 ④

0 0 0 1 <1>

$(x+1)(x+1) = x^2+x+x+1$

$= x^2+2x+1$

x^2+2x+1 | x^2+x+1 = 0

x^2+2x+1 = 0

→ Multiplication Inverse:

$x^2+x+1 \bmod m(x) = 1$

$m(x)=1$ → $x^2+x+1 \bmod 1 = x^2+x$.

→ $x^2+x+1 \bmod x = x^2+1$

→ $x^2+x+1 \bmod (x+1) = x^2$.

→ $x^2+x+1 \bmod (x^2+1) = x$.

→ $x^2+x+1 \bmod (x^2+x) = 1$

→ x | x^2+x+1 (1) → x^2+1

→ $x+1$ | x^2+x+1 (x) → x

x^2+1 | x^2+x+1 (1) = 0111 − 0101 = 0010 = x.

jadi Multiplication Inverse = (x^2+x).