Intro to Cryptography and Computer Security

Question 1

Correct

Mark 5.00 out of 5.00

Flag question

Seseorang dikatakan melakukan *active attack* jenis ....., jika ia menjalankan software yang menyebabkan server tidak dapat diakses oleh pihak-pihak yang berhak.

Answer: denial of service ✓

Question 6

Correct

Mark 5.00 out of 5.00

Flag question

Security service yang disebut ..... diperlukan dalam aplikasi e-commerce agar dapat dipastikan bahwa pelanggan tidak dapat menyangkal bahwa ia telah menyetujui suatu pembelian.

Answer: nonrepudiation ✓

Question 10

Correct

Mark 5.00 out of 5.00

Flag question

Seseorang dikatakan melakukan *attack* apa, jika ia mengulang transmisi suatu paket data dengan tujuan untuk menipu?

Select one:

- a. replay ✓
- b. masquerade
- c. eavesdropping
- d. repudiation

Classical Encryption Technique

Question 3

Complete

Mark 4.00 out of 5.00

Flag question

Pilih (sebutkan huruf di depan) sifat dari **one-time pad**. (Jawaban yang benar mungkin lebih dari satu.)

a. Unbreakable.

b. Key-nya random.

c. Key-nya harus sama panjang dengan message.

d. Key-nya hanya boleh dipakai satu kali.

e. Operasi enkripsi sama dengan dekripsi, yaitu **bitwise XOR**.

f. Ciphertext-nya random.

Sifat dari one-time pad: **a, b, c, d, e**

- a. Ubreakable
- b. Key-nya random
- c. Key-nya harus sama panjang dengan message
- d. Key-nya hanya boleh dipakai satu kali
- e. Operasi enkripsi sama dengan dekripsi, yaitu bitwise XOR

Comment:
Pilihan f juga benar.

Question 4

Complete

Mark 10.00 out of 10.00

Flag question

Lakukan **dekripsi** Vigenère terhadap ciphertext **MYBDKEIHCU** dengan kunci **DEPOK**.

Key = DEPOK = 4 5 16 15 11 dengan nilai shift = 3 4 15 14 10

Cara dekripsi:

M ==> (13 - 3) mod 26 = 10 = J

Y ==> (25 - 4) mod 26 = 21 = U

B ==> (2 - 15) mod 26 = 13 = M

D ==> (4 - 14) mod 26 = 16 = P

K ==> (11 - 10) mod 26 = 1 = A

E ==> (5 - 3) mod 26 = 2 = B

I ==> (9 - 4) mod 26 = 5 = E

H ==> (8 - 15) mod 26 = 19 = S

C ==> (3 - 14) mod 26 = 15 = O

U ==> (21 - 10) mod 26 = 11 = K

Hasil dekripsinya adalah **JUMPABESOK**

Comment:

Question 1 Not answered Marked out of 10.00

Lakukan dekripsi Vigenère terhadap ciphertext MIGEGVEIM dengan kunci KEREN.

Buat latihan ajaaa

Block Cipher and DES

Question 8

Correct

Mark 5.00 out of 5.00

Flag question

Untuk S-Box DES berikut ini:

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Input biner 110000 memberikan output biner: .....

Select one:

- a. 1111 ✓
- b. 1011
- c. 0111
- d. 0101

Question 4 Not answered Marked out of 10.00

Dengan menerapkan initialization permutation (IP) DES (Slide 3.21), hitung hasil permutasi dari ABABCDCDEFEF0202 (hex). Tulis hasil permutasi dalam bentuk hex juga.

Hitung sendiri yaa 😊

Finite Fields

Question 9

Complete

Mark 15.00 out of 15.00

Flag question

(a) [10] Cari *multiplicative inverse* dari polynomial yang direpresentasikan oleh bilangan hex {8A} untuk GF(2^8) yang dipakai AES, dengan mengisi tabel berikut menurut **Extended Euclidean Algorithm**:

q(x)	r(x)	y(x)	a(x)	b(x)	$y_2(x)$	$y_1(x)$

(b) [5] Cari representasi $x^6 + x^5 + x^3 + x^2$

sebagai pangkat dari generator **g** dalam GF(2^8) AES.

Polinomial *irreducible* yang dipakai AES adalah $x^8 + x^4 + x^3 + x + 1$.

a) multiplicative inverse dari polinomial {8A} = 1000 1010 = $x^7 + x^3 + x$ di GF(2^8) adalah sebagai berikut:

q(x)	r(x)	y(x)	a(x)	b(x)	$y_2(x)$	$y_1(x)$
-	-	-	$x^8 + x^4 + x^3 + x + 1$	$x^7 + x^3 + x$	0	1
x	$x^3 + x^2 + x + 1$	x	$x^7 + x^3 + x$	$x^3 + x^2 + x + 1$	1	x
$x^4 + x^3$	x	$x^5 + x^4 + 1$	$x^3 + x^2 + x + 1$	x	x	$x^5 + x^4 + 1$
$x^2 + x + 1$	1	$x^7 + x^4 + x^2 + 1$	x	1	$x^5 + x^4 + 1$	$x^7 + x^4 + x^2 + 1$
x	0	$x^8 + x^4 + x^3 + x + 1$	1	0	**$x^7 + x^4 + x^2 + 1$**	$x^8 + x^4 + x^3 + x + 1$

Hasilnya adalah **$x^7 + x^4 + x^2 + 1$** atau **{95}** dalam hex

Teori representasi dengan generator: Setiap polinom di GF(2^n) bisa direpresentasikan dengan generator g yang memenuhi m(g) = 0

M(g) = 0 → g^8 + g^4 + g^3 + g + 1 = 0 → g^8 = g^4 + g^3 + g + 1

b) representasi $x^6 + x^5 + x^3 + x^2$ dengan generator g:

Representasi power	Representasi polinomial
0	0
1	1
g^1	g
g^2	g^2
g^3	g^3
g^4	g^4
g^5	g^5
g^6	g^6
g^7	g^7
g^8	$g^4 + g^3 + g + 1$
g^9	$g * (g^8) = g^5 + g^4 + g^2 + g$
g^{10}	**$g * (g^9) = g^6 + g^5 + g^3 + g$**

$g^8 = g^8 \bmod g^8 + g^4 + g^3 + g + 1 = g^4 + g^3 + g + 1$, maka $g^6 + g^5 + g^3 + g^2 = g^2 (g^4 + g^3 + g + 1) = g^2 * g^8 = g^{10}$

Representasinya sebagai pangkat dari generator g adalah **g^{10}**

Question 11

Complete

Mark 20.00 out of 20.00

Flag question

(a) [10] Andaikan {AB} dan {23} adalah representasi hex dari dua unsur dalam GF(2^8) AES. Cari hasil **penjumlahan** dari kedua unsur itu. Nyatakan hasil akhir dalam representasi hex juga.

(b) [10] Andaikan {AB} dan {23} adalah representasi hex dari dua unsur dalam GF(2^8) AES. Cari hasil **perkalian** dari kedua unsur itu. Nyatakan hasil akhir dalam representasi hex juga.

a) {AB} = 1010 1011

{23} = 0010 0011

Penjumlahan = bitwise XOR

1010 1011

0010 0011

---------- +

1000 1000

Hasil penjumlahan = 1000 1000 = **{88}**

b)

{AB} = 1010 1011

{23} = 0010 0011

Perkalian = Left Shift dan XOR

Tabel perkailan:

1010 1011 * 0000 0010 = 0101 0110 XOR 0001 1011 = 0100 1101

1010 1011 * 0000 0100 = 1001 1010

1010 1011 * 0000 1000 = 0011 0100 XOR 0001 1011 = 0010 1111

1010 1011 * 0001 0000 = 0101 1110

1010 1011 * 0010 0000 = 1011 1100

1010 1011 * 0100 0000 = 0111 1000 XOR 0001 1011 = 0110 0011

1010 1011 * 1000 0000 = 1100 0110

Perkalian = {AB} * {23} =

1010 1011 * 0010 0011 =

(1010 1011 * 0010 0000) XOR (1010 1011 * 0000 0010) XOR (1010 1011 * 0000 0001) =

1011 1100 XOR 0100 1101 XOR 1010 1011 =

1111 0001 XOR 1010 1011 =

0101 1010

Hasil perkalian = 0101 1010 = **{5A}**

Question 3 Not answered Marked out of 30.00

(a) [10] Cari *multiplicative inverse* dari polynomial yang direpresentasikan oleh bilangan biner 101011 untuk GF(2^6) dengan *irreducible polynomial* x^6+x+1, dengan mengisi tabel dengan header:

q(x)	r(x)	y(x)	a(x)	b(x)	$y_2(x)$	$y_1(x)$

(b) [10] Cari representasi $x^3 + x^2$ sebagai pangkat dari generator **g** dalam GF(2^6) tersebut.

(c) [10] Andaikan 32 dan 43 adalah representasi desimal dari dua unsur dalam GF(2^6) tersebut.

Cari hasil 32/43 dalam representasi desimal. Gunakan hasil dari bagian (a).

Bagian (a)

```
q              | r              | y              | a              | b              | y2             | y1
-              | -              | -              | x6 + x + 1     | x5 + x3 + x + 1 | 0              | 1
x              | x4 + x2 + 1    | x              | x5 + x3 + x + 1 | x4 + x2 + 1    | 1              | x
x              | 1              | x2 + 1         | x4 + x2 + 1    | 1              | x              | x2 + 1
x4 + x2 + 1    | 0              | x6 + x + 1     | 1              | 0              | x2 + 1         | x6 + x + 1
GCD = x2 + 1
GCD (decimal) = 5
GCD (hex) = 0x5
Hasil perkalian: 1
```

Bagian (b)

Cara 1: Dengan perhitungan

Tinjau $M(x) = x^6 + x + 1$. Disini didapat bahwa g memenuhi $g^6 + g + 1 = 0$. Berarti $g^6 = - g – 1 = g + 1$.

Lihat $x^3 + x^2$. Dalam bentuk g, $g^3 + g^2 = g^2 (g + 1) = g^2 * g^6 = \mathbf{g^8}$

Cara 2: Dengan tabel

Representasi **g**	Polinom
0	0
1	1
g^1	g
g^2	g^2
g^3	g^3
g^4	g^4
g^5	g^5
g^6	g + 1
g^7	$g^2 + g^1$
g^8	**$g^3 + g^2$**

Didapat bahwa representasi $x^3 + x^2$ sebagai pangkat dari generator g adalah $\mathbf{g^8}$

Bagian (c)

32 / 43 = 32 * 43^-1 = 32 * 5 = 100 000 * 000 101 = 100 110

Cara:

100 000 * 000 001 = 100 000

100 000 * 000 010 = 000 000 + 000 011 = 000 011

100 000 * 000 100 = 000 110

Berarti => 100 000 * 000 101 =
100 000 * (000 100 XOR 000 001) =
(100 000 * 000 100) XOR (100 000 * 000 001) =
000 110 XOR 100 000 =
100 110

---

[20] Pilih (**lingkari** huruf di depan) **semua** jawaban yang benar (bisa lebih dari satu).

e) Polinomial yang irreducible atas GF(2):

A. $x^2 + 1$ B. $x^3 + x^2 + 1$ C. $x^4 + x$ D. $x^5 + x^4 + x^3 + x + 1$

Mencari irreducible sama saja seperti mencari bilangan prima, yaitu **polinomnya tidak mempunyai faktor lain selain dirinya sendiri dan 1 di GF(2)**.

- Pilihan A: $x^2 + 1$ reducible ➔ Faktor lain: $x + 1$
- **Pilihan B: $x^3 + x^2 + 1$ irre*ducib*le**
- Pilihan C: $x^4 + x$ reducible ➔ Faktor lain: x dengan $x^3 + 1$
- **Pilihan D: $x^5 + x^4 + x^3 + x + 1$ irreducible**

---

j) $GF(2^8)$ mempunyai order:

A. 8
B. 16
C. 64
D. 256

Order = 2^8 = 256

AES

Question 2

Complete

Mark 10.00 out of 10.00

Flag question

Lakukan operasi perkalian matriks di bawah ini, dalam tahap MixColumns pada AES untuk menghasilkan byte ($s'_{2,0}$). Ingat indeks mulai dari 0.

Perlihatkan langkah-langkah menurut cara SHIFT dan XOR.

02	03	01	01		34	C8	E5	12
01	02	03	01	×	BA	90	AB	FD
01	01	02	03		CD	EF	12	36
03	01	01	02		E1	56	78	90

$s'_{2,0}$=.....

$s'_{2,0}$ = 01 * 34 + 01 * BA + 02 * CD + 03 * E1 = 34 + BA + 81 + 38 = **37**

Perhitungan:

- **01 * 34 =** 0000 0001 * 0011 0100 = 0011 0100 = **34**
- **01 * BA =** 0000 0001 * 1011 1010 = 1011 1010 = **BA**
- **02 * CD =** 0000 0010 * 1100 1101 = 1001 1010 XOR 0001 1011 = 1000 0001 = **81**
- **03 * E1 =** 0000 0011 * 1110 0001 = 0000 0010 * 1110 0001 + 0000 0001 * 1110 0001 = 1100 0010 XOR 0001 1011 XOR 1110 0001 = 1101 1001 XOR 1110 0001 = 0011 1000 = **38**
- **34 + BA + 81 + 38 =** 0011 0100 XOR 1011 1010 XOR 1000 0001 XOR 0011 1000 = 1000 1110 XOR 1000 0001 XOR 0011 1000 = 0000 1111 XOR 0011 1000 = 0011 0111 = **37**

Question 7

Complete

Mark 10.00 out of 10.00

Flag question

Untuk AES, cari round-key untuk round ke-2 (j=2), yaitu w_8, w_9, w_{10}, dan w_{11}, apabila round-key untuk round ke-1 dalam notasi hex adalah

A0 A0 A0 A0 B1 B1 B1 B1 C2 C2 C2 C2 D3 D3 D3 D3.

W_4 = A0 A0 A0 A0

W_5 = B1 B1 B1 B1

W_6 = C2 C2 C2 C2

W_7 = D3 D3 D3 D3

$G(w_7)$:

- RotWord(w_7) = D3 D3 D3 D3
- SubWord(w_7) = 66 66 66 66
- Rcon(2) = 02 00 00 00
- $G(w_7)$ = Rcon(2) XOR SubWord(w_7) = 64 66 66 66

W_8 = $g(w_7)$ XOR w_4 = 64 66 66 66 XOR A0 A0 A0 A0 = C4 C6 C6 C6 C6

W_9 = w_8 XOR w_5 = C4 C6 C6 C6 XOR B1 B1 B1 B1 = 75 77 77 77

W_{10} = w_9 XOR w_6 = 75 77 77 77 XOR C2 C2 C2 C2 = B7 B5 B5 B5

W_{11} = w_{10} XOR w_7 = B7 B5 B5 B5 XOR D3 D3 D3 D3 = 64 66 66 66

Round key untuk round ke-2 adalah C4 C6 C6 C6 C6 75 77 77 77 B7 B5 B5 B5 64 66 66 66

Modes of Operations for Block Cipher

Question 5

Complete

Mark 10.00 out of 10.00

Flag question

Perhatikan plaintext berikut ini yang terdiri dari 20 byte dalam notasi hex. Lakukan padding menurut skema padding PKCS#5 untuk block-cipher dengan ukuran block 128 bit.

88 C1 AB 32 C7 02 CC EF 5F 67 9A 4A BB 23 49 16 50 7F 25 C0

ukuran block = 128 bit = 16 byte

plain text = 20 byte

Block 1 = 88 C1 AB 32 C7 02 CC EF 5F 67 9A 4A BB 23 49 16

Block 2 = 50 7F 25 C0

Dapat dilihat bahwa block 2 kurang 16 - 4 = 12 bytes, sehingga 12 bytes sisanya akan di-padding dengan bytes bernilai 12 = 0C saat menggunakan skema PKCS#5. Hasil dari block 2 setelah dilakukan padding adalah **50 7F 25 C0 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C**

Hasil keseluruhan plaintext setelah di padding adalah = **88 C1 AB 32 C7 02 CC EF 5F 67 9A 4A BB 23 49 16 50 7F 25 C0 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C**

Number Theory for PKC

a) Nilai dari fungsi totient Euler $\phi(16)$ adalah

A. 7 B. 8 C. 10 D. 15

Jawab: 16 * (1 – ½) = 8

```
initial: 16
remaining= 8 prime= 2
remaining= 4 prime= 2
remaining= 2 prime= 2
2 is already prime
factor= [2, 2, 2, 2]
Totient value for 16 is 8.0
```

Hitung nilai dari fungsi totient Euler $\varphi(500)$.

Jawab:

```
initial: 500
1 : remaining= 250 prime= 2
1 : remaining= 125 prime= 2
1 : remaining= 25 prime= 5
1 : remaining= 5 prime= 5
5 is already prime
factor= [2, 2, 5, 5, 5]
Totient value for 500 is 200.0
```

Cari dua digit terakhir dari 3^{2007} dengan menggunakan Teorema Euler.

Jawab:

```
initial: 100
remaining= 50 prime= 2
remaining= 25 prime= 2
remaining= 5 prime= 5
5 is already prime
factor= [2, 2, 5, 5]
Totient value for 100 is 40.0
result: 87
```

Karena totient value dr 100 = 40, maka 3^40 = 1

3^2007 = 3^2000 * 3^7 = (3^40)^50 * 3^7 = 1 * 3^7 = 21**87**

---

4. Terapkan algoritma Miller-Rabin untuk mengecek primality dari bilangan-bilangan n berikut ini.
   a) n = 29 dengan memilih a = 10 Maybe prime
   b) n = 29 dengan memilih a = 2 Maybe prime
   c) n = 221 dengan memilih a = 21 Maybe prime
   d) n = 221 dengan memilih a = 5 Composite

PKC and RSA

f) Si X ingin mengirimkan pesan rahasia kepada si Y dengan menggunakan sistem kripto asimetrik.

A. Si X mengenkripsi pesan itu dengan menggunakan kunci rahasia si X.
B. Si X mengenkripsi pesan itu dengan menggunakan kunci umum si X.
C. Si X mengenkripsi pesan itu dengan menggunakan kunci rahasia si Y.
D. Si X mengenkripsi pesan itu dengan menggunakan kunci umum si Y.

Jawab: D

---

5. Angelina dan Brad berkomunikasi dengan sistem kripto RSA basic. Brad memilih secara rahasia dua bilangan prima: p = 5 dan q = 11. Brad mengumumkan bahwa kunci publiknya adalah (e=27, n=55).

a) Cari kunci rahasia Brad dengan *Euclid's Extended Algorithm.*

Jawab:

q	r	y	a	b	y2	y1
-	-	-	40	27	0	1
1	13	-1	27	13	1	-1
2	1	3	13	1	-1	3
13	0	-40	1	0	3	-40

```
Multiplicative inverse = 3

Public Key = (27, 55)
Private Key = (3, 55)
```

b) Brad mendapat pesan dari Angelina, yaitu **20**. Dekripsikan pesan itu.
Decrypt dgn private key

Jawab:

d * e == 1 (mod totient(p*q)) → d . 27 == 1 (mod totient(55)) → **d . 27 == 1 (mod 40) → Cara cari d adal cari inverse multiplikatif dari 27 dalam dunia mod 40 → EEA**

i	bi	c	d
1	1	1	20
0	1	3	25

```
Hasil modulo = 25
Decrypted Message:  25
```

Dekripsi → M = C ^ d mod n → M = 20 ^ 3 mod 55 = 25

c) Brad mau membuat tandatangan digital untuk pesan **15** sehingga orang lain (termasuk Angelina) dapat yakin bahwa pesan itu berasal dari Brad. Buat tandatangan digital itu (tanpa fungsi hash).
Enkrip dgn private key

Jawab:

i	bi	c	d
1	1	1	15
0	1	3	20

```
Hasil modulo = 20
Ciphertext:  20
```

Saat pesan diterima Angelina, Angelina dapat cek digital signature dan ambil pesan dengan cara dekipri menggunakan public key Brad:

i	bi	c	d
4	1	1	20
3	1	3	25
2	0	6	20
1	1	13	25
0	1	27	15

Hasil modulo = 15

Decrypted Message: 15

---

3. Hitung 3^{1668} **mod 22** dengan algoritma Fast Modular Exponentiation.

i	10	9	8	7	6	5	4	3	2	1	0
b_i											
c											
d											

i	bi	c	d
10	1	1	3
9	1	3	5
8	0	6	3
7	1	13	5
6	0	26	3
5	0	52	9
4	0	104	15
3	0	208	5
2	1	417	9
1	0	834	15
0	0	1668	5

Hasil modulo = 5

Diffie-Hellman Protocol and ECC

g) Contoh sistem kripto yang keamanannya tergantung pada kesulitan pemecahan **problem logaritma diskret**:
   A. AES
   B. El Gamal
   C. RSA
   D. Diffie-Hellman

---

3. (a) [10] Tinjau grup $Z_{13}^{*} = (\{1,2,3,4,5,6,7,8,9,10,11,12\},*)$ yang operasinya adalah **perkalian mod 13**. Grup ini berguna untuk perhitungan-perhitungan pada kurva eliptik berikutnya.

   Lengkapi tabel operasi dan tabel inverse di bawah ini.

*	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	3	5	7	9	11
3	3	6	9	12	2	5	8	11	1	4	7	10
4	4	8	12	3	7	11	2	6	10	1	5	9
5	5	10	2	7	12	4	9	1	6	11	3	8
6												
7												
8												
9												
10												
11												
12												

a	a^{-1}
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

Invers = 1 <> 1, 2 <> 7, 3 <> 9, 4 <> 10, 5 <> 8, 6 <>11, 12 <> 12

(b) [10] Cari semua titik pada kurva elliptik $E_{13}(2,5)$.

Kalo sampai slide 42, ini harusnya udh masuk bahan UTS

Elliptic curve Ep(a, b) thd Zp → y^2 mod p = (x^3 + ax +b) mod p. Himpunan E(A, b) adalah semua pasangan bil bulan (x, y) yang memenuhi persamaan y^2 mod p = (x^3 + ax +b) mod p.

Contoh: (1, 2) anggota dari E5(4, 4) karena 2^2 mod 5 = 4 =(1^3 + 4 + 4) mod 5

Untuk soal, p = 13, a = 2, b = 5
Kolom kedua untuk mencari y^2

x	X^3 + 2x + 5 == y^2 (mod 13)	y	Titik
0	5	-	-
1	8	-	-
2	4	2, 11	(2, 2), (2, 11)
3	12	5, 8 → Lihat lookup table y^2	(3, 5), (3, 8)

4	12	5, 8	(4, 5), (4, 8)
5	10	6, 7	(5, 6), (5, 7)
6	12	5, 8	(6, 5), (6, 8)
7	11	-	-
8	0	0	(8, 0)
9	11	-	-
10	11	-	-
11	6	-	-
12	2	-	-

Tabel y^2

Y	Y^2 mod 13
0	0
1	1
2	4
3	9
4	3
5	12
6	10
7	10
8	12
9	3
10	9
11	4
12	1

---

h) Diketahui 3 adalah salah satu akar primitif dari 17. Akar-akar primitif lain dari 17 adalah
A. 5 B. 6 C. 7 D. 10

```
1   | [1]
2   | [2, 4, 8, 16, 15, 13, 9, 1]
3   | [3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1]
4   | [4, 16, 13, 1]
5   | [5, 8, 6, 13, 14, 2, 10, 16, 12, 9, 11, 4, 3, 15, 7, 1]
6   | [6, 2, 12, 4, 7, 8, 14, 16, 11, 15, 5, 13, 10, 9, 3, 1]
7   | [7, 15, 3, 4, 11, 9, 12, 16, 10, 2, 14, 13, 6, 8, 5, 1]
8   | [8, 13, 2, 16, 9, 4, 15, 1]
9   | [9, 13, 15, 16, 8, 4, 2, 1]
10  | [10, 15, 14, 4, 6, 9, 5, 16, 7, 2, 3, 13, 11, 8, 12, 1]
11  | [11, 2, 5, 4, 10, 8, 3, 16, 6, 15, 12, 13, 7, 9, 14, 1]
12  | [12, 8, 11, 13, 3, 2, 7, 16, 5, 9, 6, 4, 14, 15, 10, 1]
13  | [13, 16, 4, 1]
14  | [14, 9, 7, 13, 12, 15, 6, 16, 3, 8, 10, 4, 5, 2, 11, 1]
15  | [15, 4, 9, 16, 2, 13, 8, 1]
16  | [16, 1]
Primitive roots: [3, 5, 6, 7, 10, 11, 12, 14]
```

---

6. [10] A dan B menggunakan teknik pertukaran kunci Diffie-Hellman dengan ***common prime*** q = 79 dan ***akar primitif*** α = 6.

   Nilai-nilai dari $\mathbf{6^i \bmod 79}$ untuk i = 1, 2, ..., 78 adalah sebagai berikut:

   6 36 58 32 34 46 39 76 61 50

   63 62 56 20 41 9 54 8 48 51

   69 19 35 52 75 55 14 5 30 22

   53 2 12 72 37 64 68 13 78 73

   43 21 47 45 33 40 3 18 29 16

   17 23 59 38 70 25 71 31 28 10

   60 44 27 4 24 65 74 49 57 26

   77 67 7 42 15 11 66 1

   a) Jelaskan bahwa 6 memang sebuah akar primitif dari 79.
   b) Tentukan nilai logaritma diskret $\mathbf{dlog_{6,79}(71)}$.
   c) Jika A mempunyai kunci privat $X_A = 56$, cari kunci publik Y_A.
   d) Jika B mempunyai kunci privat $X_B = 22$, cari kunci publik Y_B.
   e) Cari ***kunci rahasia bersama*** dari A dan B.

Jawab:

a) Pangkat dari 6 menghasilkan bilangan berbeda dari 1 – 78 saat di modulo 79

b) $dlog_{6,79}(71) = \ldots$ ➔ 6^ i mod 79 = 71, i = ...
c) YA = $alpha^{XA}$ mod q = 6^56 mod 79 = ...
d) YB = $alpha^{XB}$ mod q = 6^22 mod 79 = ...
e) Kunci rahasia bersama: alpha ^(XA * XB) mod q = $6^{56 * 22}$ mod 79 = ...

---

2. Sistem Kripto **ElGamal**, yang merupakan pengembangan dari teknik Diffie-Hellman, bekerja sebagai berikut:
   - Parameter umum (berlaku untuk semua user)
     sebuah bilangan prima random p dan sebuah akar primitif α dari p.
   - Pembuatan kunci
     Untuk membuat kuncinya, user A melakukan langkah-langkah:
     1. pilih kunci privat x berupa sebuah bilangan random yang lebih kecil dari p;
     2. hitung kunci publik $y := \alpha^x \pmod p$;
   - Enkripsi
     Untuk mengirim plaintext rahasia $m < p$ kepada user A, pengirim B memilih sebuah bilangan random $k < p$ dan membuat ciphertext berupa pasangan (c_1,c_2) sebagai berikut:
     $c_1 := \alpha^k \pmod p$
     $c_2 := y^k m \pmod p$
   - Dekripsi
     Untuk mendekripsi ciphertext (c_1,c_2), user A melakukan perhitungan:
     $m := c_2 (c_1^x)^{-1} \pmod p$
     Perhatian: pangkat -1 di sini berarti invers perkalian mod p.

   a) Buktikan bahwa proses dekripsi itu memang menghasilkan plaintext m.

   b) Ami dan Bob menggunakan sistem kripto ElGamal dengan bilangan prima random p = 11 dan akar primitif α yang dipilih dari dua bilangan: 4 atau 7. Satu dari dua bilangan ini adalah akar primitif dari 11, yang lainnya bukan. Tentukan α.

   c) Setelah memilih kunci privatnya, Ami mendapatkan kunci publiknya yaitu 10 dan mengumumkannya. Cari kunci privat Ami.

   d) Ami mendapat kiriman ciphertext dari Bob yaitu sepasang bilangan (2, 3). Cari plaintext-nya. Plaintext ini merupakan tanggal si Bob akan melamar si Ami. Sayangnya bulan dan tahun belum diketahui.

---

1. Cari semua akar primitif dari 13, mulai dari yang terkecil. Ada berapa banyak akar primitif dari 13?

2. Cari semua titik pada kurva elliptik $\mathbf{E_{11}(1,6)}$ dengan membuat sebuah tabel. Selain titik **O** yang terletak di ∞, titik-titik yang terletak pada $E_{11}(1,6)$ dapat diperoleh dengan memberi x nilai 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, dan 10 (karena **mod 11**) dan mencoba mencari apakah ada nilai untuk y.
