FAST EXPONENTIATION

1. Konsep Modulo
2. Perpangkatan Cepat

Fast Exponentiation

- Algoritma kunci-publik seperti RSA, Elgamal, Rabin-Williams Cryptosystem, DSA, dan sebagainya, sederhana dalam perhitungannya namun sulit dalam implementasinya dalam perangkat lunak. Hal ini karena algoritma tersebut melakukan operasi perpangkatan dengan bilangan yang besar.
- Metode *Fast Exponentiation* digunakan untuk menghitung operasi pemangkatan besar bilangan bulat modulo dengan cepat.

Konsep Modulo (1)

- Konsep Modulo merupakan bagian yang dibahas pada Matematika Diskret.
- Operasi modulo, misal: ***a* mod *b* = *c*** mempersyaratkan nilai-nilai *a, b,* dan *c* harus integer (bulat), dengan *c* merupakan sisa hasil-bagi bulat dari *a*/*b* → div *(a*/*b)*
- Contoh: 10/3 = 3, sisa 1 → maka 10 mod 3 = 1
- Penggunaan kalkulator yang tidak ada fungsi **mod**-nya

  contoh: Berapa 124 mod 5?

  cara: 124 : 5 = 24.8

  24 _

  0.8

  0.8*5 = 4

  Sehingga, 124 mod 5 = 4, atau bisa ditulis: 124 ≡ 4 mod 5

Konsep Modulo (2)

- Jika a mod b, dengan $a < b$, maka a mod $b = a$
- Jika a mod b, dengan $a > b/2$ dan $a < b$ maka a mod $b = a-b = -(b-a)$

Contoh: berapakah 31 mod 33?

Jawab: $a = 31$, $b = 33$, dengan $a < b$ (=31 < 33), sekaligus

$a > b/2$ (= 31 > 33/2 = 16,5), maka dapat dituliskan:

31 mod 33 = 31 $\equiv$ 31-33 $\equiv$ -2 mod 33

atau dapat ditulis: 31 $\equiv$ 31-33 $\equiv$ -2 mod 33

yang merupakan cara penulisan cepat.

Angka hasil modulo yang kecil lebih disukai → lebih mudah penghitungannya pada *fast exponentiation.*

Model penulisan lain (lebih panjang):

31 mod 33 = (31-33) mod 33 = -2 mod 33 = -2

FAST EXPONENTIATION

$$3^{11}\ mod\ 35 =$$

$$11 = 8 + 2 + 1$$

$$= 2^3 + 2^2 + 2^1$$

$$3^{11} = (3^8)(3^2)(3^1)$$

$$3^1 \equiv 3\ mod\ 35$$

$$3^2 \equiv 9\ mod\ 35$$

$$3^4 \equiv (3^2)^2 \equiv 9^2 \equiv 81 \equiv (2 * 35) + 11 = 11\ mod\ 35$$

$$3^8 \equiv (3^4)^2 \equiv 11^2 \equiv 121 \equiv (3 * 35) + 16 = 16\ mod\ 35$$

- Jadi hasil dari 3^{11} mod 35

$$3^{11} \equiv (16)(9)(3) \equiv 432 \equiv (12 * 35) + 12 = 12\ mod\ 35$$

- Contoh

$10^{98} \bmod 11$

$10^{98} \bmod 11 \equiv 10^{64+32+2}$

$10 \bmod 11 \equiv 10 \equiv (-1) \bmod 11$

$10^2 \equiv (-1)^2 \equiv 1 \bmod 11$

$10^{32} \equiv (10^2)^{16} = 1^{16} \equiv 1 \bmod 11$

$10^{64} \equiv (10^{32})^2 = 1^2 \equiv 1 \bmod 11$

Jadi $10^{98} \bmod 11 \equiv 10^{64+32+2} \equiv 10^{64}. 10^{32}. 10^2$

$\equiv (1). (1). (1) \equiv$ **1 mod 11**

- $572^{37} \bmod 713$

$572^{37} = 572^{32} \cdot 572^{4} \cdot 572$

$572 \bmod 713 \equiv 572 \equiv (-141) \bmod 713$

$572^{2} \equiv (-141)^{2} \equiv 630 \equiv (-83) \bmod 713$

$572^{4} \equiv (572^{2})^{2} \equiv (-83)^{2} \equiv 472 \equiv (-241) \bmod 713$

$572^{8} \equiv (572^{4})^{2} \equiv (-241)^{2} \equiv 328 \bmod 713$

$572^{16} \equiv (572^{8})^{2} \equiv 328^{2} \equiv 634 \equiv (-79) \bmod 713$

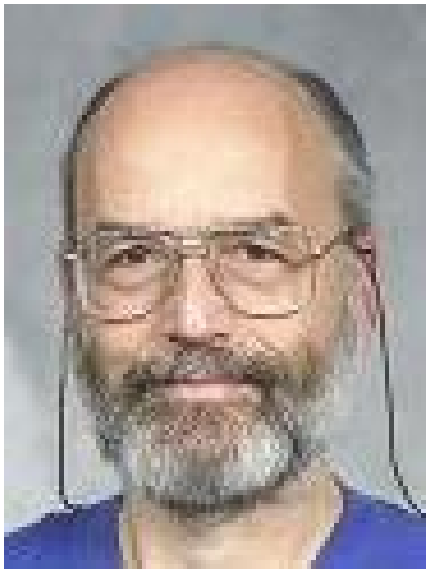
$572^{32} \equiv (572^{16})^{2} \equiv (-79)^{2} \equiv 537 \equiv (-176) \bmod 713$

Jadi $572^{37} \bmod 713 \equiv 572^{32} \cdot 572^{4} \cdot 572 \equiv$

$(-176).(-241).(-141) \equiv$ **(-12) mod 713**

ENKRIPSI RSA DAN EL GAMAL

Dr. R. Rizal Isnanto, S.T., M.M., M.T.

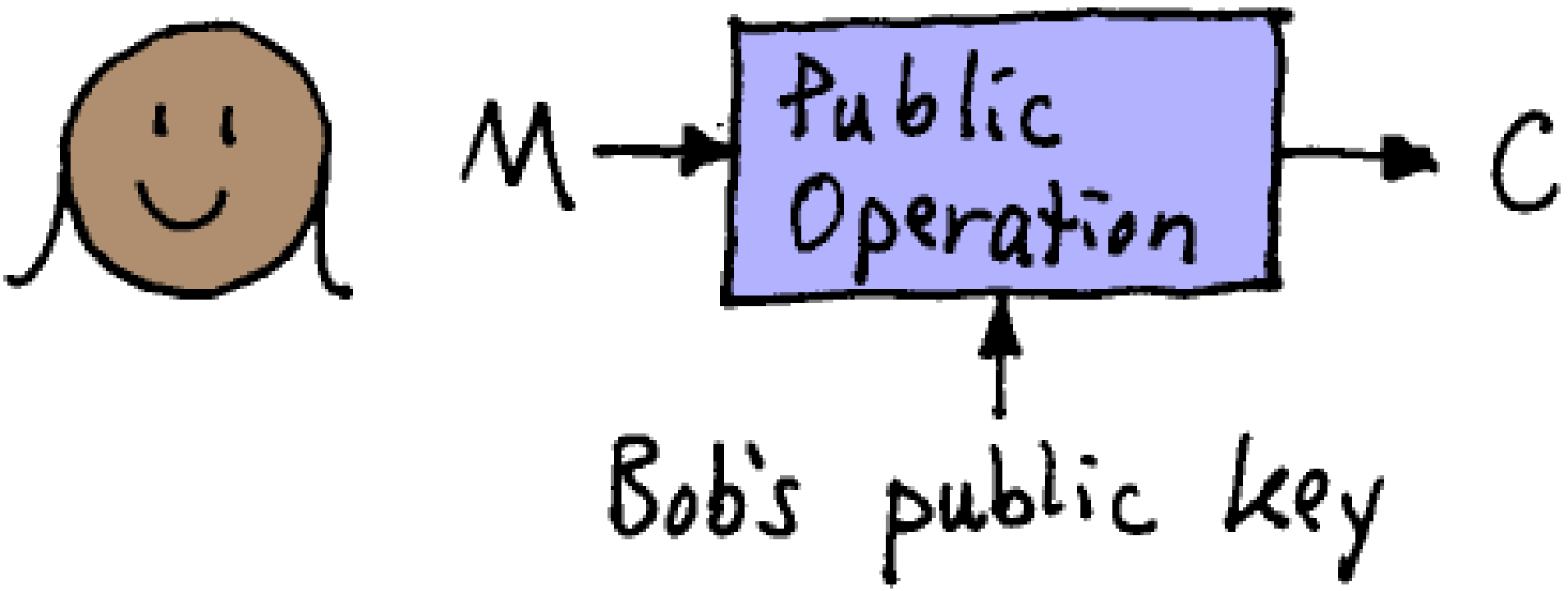




R S A

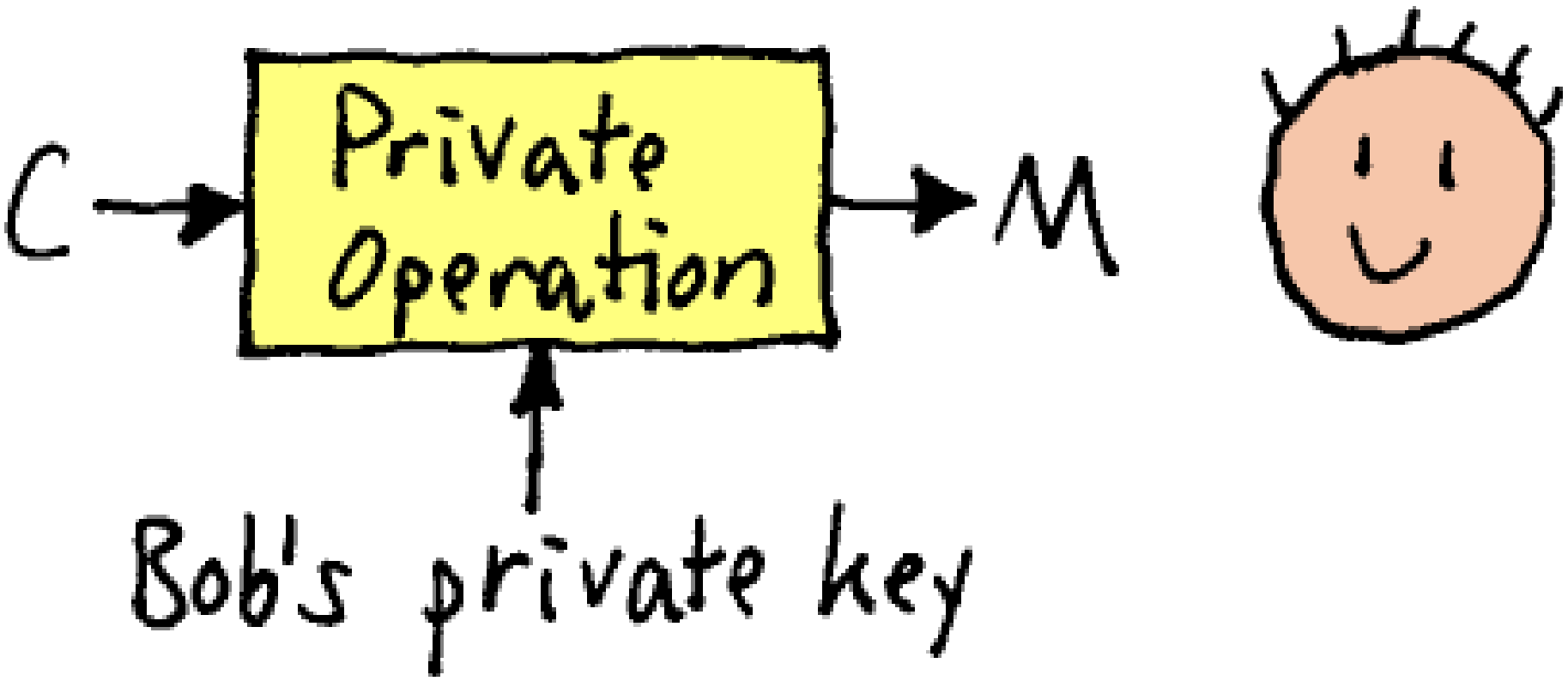
Ronald Rivest, Adi Shamir, Leonard Adleman)

RSA PUBLIC KEY ALGORITHM

Everyone knows Bob's public key.
Anyone can do the public operation.



Only Bob knows his own private key.
It is not possible to find *M*, given only *C* and not the private key.
It is not possible to find the private key, given the public key.
Therefore, only Bob can do the private operation.



Ide Utama Enkripsi RSA (Rivest, Shamir, Adleman)

1. Key setup

- Pilih dua buah bilangan prima p,q
- Hitung n = p.q
- Pilih e sedemikian hingga $1<e<\phi$
  dengan $\phi = (p-1)(q-1)$
- Hitung d yang secara relatif prima terhadap ϕ

kunci publik (n,e)
kunci privat (d)

2. Enkripsi

$c = m^e \bmod n$

m = pesan asli / plaintext

3. Dekripsi

$m = c^d \bmod n$

contoh soal

1. Diketahui pada algoritma RSA bahwa key setup yang dilakukan adalah p=3, q=11 dan e dipilih 17

a. Berapa nilai d yang dipilih ?

b. Jika m=5 tentukan cipher teksnya !

c. Buktikan bahwa dekripsi yang dilakukan akan menghasilkan m yang sesuai butir b !

Jawab:

p=3 q=11

n=p.q=(3)(11)=33

ϕ=(p-1)(q-1)=(2)(10)=20

e 1<e<ϕ 1<e<20

misal e=17

pilih d, 1<d< ϕ ed=1 mod ϕ

Kandidat d	**e.d**	**e.d mod ϕ**	**keterangan**
2	34	34 mod 20 = 14	bukan
3	51	51 mod 20 = 11	Bukan
4	68	68 mod 20 = 8	Bukan
….	…	…	…
13	221	221 mod 20 = 1	Dipilih

- kunci publik (n,e)=(33,17)
- kunci privat (d)=(13)

b. Enkripsi

c = m^e mod n m=5

$$5^{17}\ mod\ 33 =$$

$$5^{17} = (5^{16})(5^{1})$$

$$5^{1} = 5\ mod\ 33$$

$$5^{2} \equiv 25 = -8\ mod\ 33$$

$$5^{4} \equiv 64 \equiv (33 * 1) + 31 \equiv 31 = -2\ mod\ 33$$

$$5^{8} \equiv 4 = 4\ mod\ 33$$

$$5^{16} \equiv 16 = 16\ mod\ 33$$

$$c = (5^{16})(5^{1})$$

$$c = (16)(5) \equiv 80 \equiv (2 * 33) + 14 \equiv 14\ mod$$

❖ c=14

c. Dekripsi

$m = c^d \ mod \ n$

$m = 14^{13} \ mod \ 33$

$m = 14^{13} = (14^8)(14^4)(14^1)$

$14^1 = 14 \ mod \ 33$

$14^2 \equiv 196 \equiv (33 * 5) + 31 \equiv 31 = -2 \ mod \ 33$

$14^4 = 4 \ mod \ 33$

$14^8 = 16 \ mod \ 33$

$m \equiv (14^8)(14^4)(14^1)$

$\equiv (16)(4)(14) \equiv 896 \equiv (33 * 27) + 5 = 5 \ mod \ 33$

❖ m = 5 (terbukti)

PR (1 minggu)

Diketahui pada algoritma RSA bahwa *key setup* yang dilakukan adalah p=13, q=17, dan e dipilih = 25.

a. Berapa nilai d yang dipilih? (d adalah ganjil sedemikian hingga $159 < d < 190$)

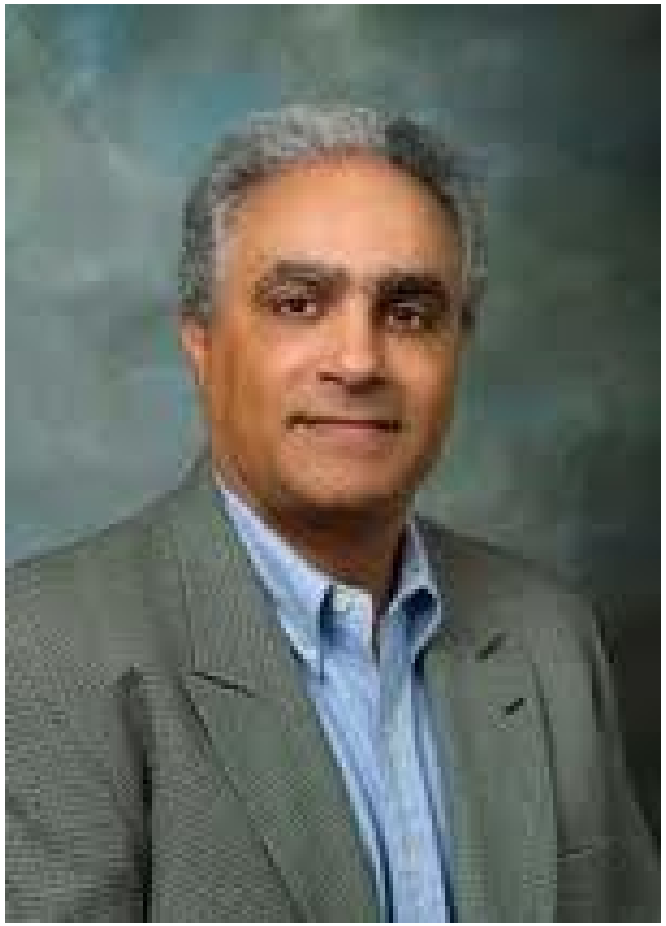
b. Jika $m = 7$, tentukan *ciphertext* c-nya.

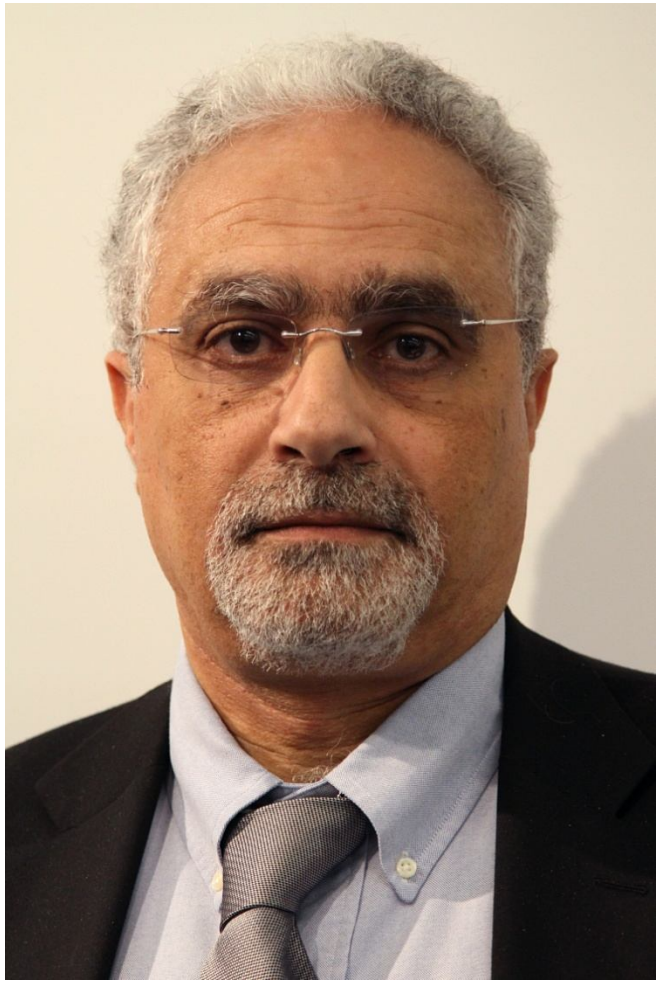
c. Buktikan bahwa dekripsi yang dilakukan

akan menghasilkan m sesuai butir b.

El Gamal Encryption

- Diambil dari nama penggagasnya: Taher Elgamal (Mesir)





Ide Utama Enkripsi El Gamal

1. Key setup

a. Tentukan bilangan prima p

b. hitung α sedemikian hingga $1 < \alpha \leq p-1$

$$\alpha^{(p-1)/2} \neq 1 \bmod p$$

c. pilih a sedemikian hingga $1 \leq a \leq p-2$

hitung $\alpha^a \bmod p$

kunci publik (α, p, $\alpha^a \bmod p$)

kunci privat a

2. Enkripsi

Pesan m dengan kisaran {0,1, … , p-1}

a. Pilih bilangan bulat k, $1 \leq k \leq p-2$

b. Hitung $\gamma = \alpha^k \bmod p$ dan $\delta = m(\alpha^a)^k \bmod p$

pasangan chiperteks $c=(\gamma,\delta)$

3. Dekripsi

- Hitung $\gamma^{p-1-a} \equiv \gamma^{-a} \equiv \alpha^{-ak} \bmod p$
- Kemudian tentukan $m = \delta(\gamma^{p-1-a}) \bmod p$

- Fermat's Little Theorem: $a^{p-1} \equiv 1 \bmod p$

  untuk semua $1 < a < p$, dengan p bil. prima

contoh soal

Pada metode El gamal prima p yang dipilih adalah 23

a. Tentukan α yang sesuai

b. Jika kunci rahasia yang dipilih adalah a=7 dan k=6 tentukan chiperteks c sebagai hasil enkripsi dari m=9

c. Buktikan hasil dekripsi yang dilakukan akan menghasilkan m sesuai butir b

jawab

a. p = 23

mencari α untuk $1 < \alpha < 23$ 2,3,4,…,22

coba coba $\alpha^{(p-1)/2} \neq 1 \bmod p$

$\alpha = 2$ $2^{11} \bmod 23 = 1 \bmod 23$

$\alpha = 3$ $3^{11} \bmod 23 = 1 \bmod 23$

$\alpha = 4$ $4^{11} \bmod 23 = 1 \bmod 23$

$\alpha = 5$ $5^{11} \bmod 23 = -1 \bmod 23$ dipilih $\alpha = 5$

b. a=7 k=6 m=9

c = (γ, δ)

$\gamma = \alpha^k \bmod p = 5^6 \bmod 23 = 8 \bmod 23$ $\gamma=8$

$\delta = m\ (\alpha^a)^k \bmod p = 9\ (5^7)^6 \bmod 23 = 16 \bmod 23$ $\delta=16$

c = (γ, δ) = (8,16)

c. dekripsi

$m = \delta (\gamma^{p-1-a}) \bmod 23$

$= 16 (8^{15}) \bmod 23$

$= 9$

terbukti m = 9

PR (1 minggu)

1. Pada metode El Gamal, prima *p* yang dipilih adalah 19.
   a. Tentukan α yang sesuai.
   b. Jika kunci rahasia yang dipilih $a = 5$, dan $k = 4$, tentukan *ciphertext c* sebagai hasil enkripsi dari $m = 8$.
   c. Buktikan bahwa dekripsi yang dilakukan akan menghasilkan *m* sesuai butir

PR:

2. Dengan menggunakan rumus-rumus yang ada, buktikan bahwa:

$$\delta(\gamma^{p-1-a}) \bmod p = m$$

3. Pada metode El Gamal, prima *p* yang dipilih adalah 29.

   a. Tentukan α yang sesuai, dengan syarat

   b. Jika kunci rahasia yang dipilih $a = 7$, dan $k = 6$, tentukan ciphertext *c* sebagai hasil enkripsi dari $m = 9$.

   c. Buktikan bahwa dekripsi yang dilakukan akan menghasilkan *m* sesuai butir b.

TERIMA KASIH