Kriptografi

TK13029
COMPUTATION II

Review Teori Bilangan

Pembagian

- Jika a dan b adalah bilangan bulat dimana $a \neq 0$, dikatakan a membagi habis b jika ada bilangan bulat c sehingga $b = ac$.
  - a disebut sebagai faktor atau pembagi b
  - b disebut kelipatan dari a
  - $a \mid b$: a membagi b
  - $a \nmid b$: a tidak membagi b
  - Jika $a \mid b$ dan $a \mid c$, maka $a \mid (b + c)$
  - Jika $a \mid b$, maka Jika $a \mid bc$, untuk semua bilangan bulat c
  - Jika $a \mid b$ dan $b \mid c$, maka $a \mid c$
- Contoh: $3 \mid 7$ dan $3 \mid 12$
  - $3 \nmid 7$ dan $3 \mid 12$

Algoritma Pembagian

- Diketahui a adalah bilangan bulat dan d bilangan bulat positif. Terdapat bilangan bulat unik q dan r, dengan $0 \leq r < d$, sehingga $a = dq + r$
  - a adalah bilangan yang dibagi (*dividen*)
  - d adalah pembagi (*divisor*)
  - q adalah hasil bagi (*quotient*)
  - r adalah sisa bagi (*reminder*)
  - $q = a \operatorname{div} d$ dan $r = a \bmod d$
- Contoh: tentukan
  - q dan r untuk 101 dibagi 11
    - $101 = 11(9) + 2$, $q = 9$ dan $r = 2$
  - q dan r untuk -11 dibagi 3
    - $-11 = 3(-4) + 1$, $q = -4$ dan $r = 1$ (r tidak boleh negatif karena $0 \leq r < 3$)

Modular Arithmetic (1)

- Jika a dan b adalah bilangan bulat dan m bilangan bulat positif, maka a dikatakan kongruen b modulo m jika m membagi $a - b$.
  - a kongruen b modulo m : $a \equiv b (\mathrm{mod}\ m)$
  - a tidak kongruen b modulo m : $a \not\equiv b (\mathrm{mod}\ m)$
  - $a \equiv b (\mathrm{mod}\ m)$ jika dan hanya jika $a \bmod m = b \bmod m$
  - $a \equiv b (\mathrm{mod}\ m)$ jika dan hanya jika terdapat bilangan bulat k sehingga $a = b + km$
- Contoh:
  - apakah 17 kongruen 5 modulo 6?
    - 6 membagi habis (17 - 5) = 12
  - apakah 24 kongruen 14 modulo 6?
    - 6 tidak membagi habis (24 - 14) = 10

Modular Arithmetic (2)

- Diketahui m bilangan bulat positif. Jika $a \equiv b (\mathrm{mod}\, m)$ dan $c \equiv d (\mathrm{mod}\, m)$, maka
  - $a + c \equiv b + d (\mathrm{mod}\, m)$
  - $ac \equiv bd (\mathrm{mod}\, m)$
  - $(a + b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$
  - $ab \bmod m = \big((a \bmod m)(b \bmod m)\big) \bmod m$

Modular Exponentiation

- Menghitung

$$b^n \bmod m$$

- Konsep

$$n = (a_{k-1}a_{k-2} \ldots a_1 a_0)_2$$

$$b^n = b^{a_{k-1}\cdot 2^{k-1}+\cdots+a_1\cdot 2+a_0}$$

$$= b^{a_{k-1}\cdot 2^{k-1}} \cdot \ldots \cdot b^{a_1\cdot 2} \cdot b^{a_0}$$

Contoh: 3^{11}

$11 = (1011)_2$

$3^{11} = 3^{1\cdot 8} \cdot 3^{0\cdot 4} \cdot 3^{1\cdot 2} \cdot 3^1$

$= 3^8 \cdot 3^0 \cdot 3^2 \cdot 3^1$

$= 6561 \cdot 1 \cdot 9 \cdot 3 = 177147$

ALGORITHM 5 Fast Modular Exponentiation.

procedure *modular exponentiation*(b: integer, $n = (a_{k-1}a_{k-2} \ldots a_1 a_0)_2$, m: positive integers)

$x := 1$

$power := b \bmod m$

for $i := 0$ **to** $k - 1$

  if $a_i = 1$ **then** $x := (x \cdot power) \bmod m$

  $power := (power \cdot power) \bmod m$

return x {x equals $b^n \bmod m$}

Modular Exponentiation

- Contoh: 3^{11} **mod** 13

  $11 = (1011)_2, x = 1,$
  $power = 3$ **mod** $13 = 3$

  $a_0 = 1, x = (1 \cdot 3)$**mod** $13 = 3,$
  $power = 3 \cdot 3$ **mod** 13
  $= 3^2$ **mod** 13
  $= 9$ **mod** 13
  $= 9$

  $a_1 = 1, x = (3 \cdot 9)$**mod** $13 = 1,$
  $power = 81$ **mod** $13 = 3$

  $a_2 = 0, x = 1,$
  $power = 9$ **mod** $13 = 9$

  $a_3 = 1, x = (1 \cdot 9)$**mod** $13 = 9,$
  $power = 81$ **mod** $13 = 3$

  Jadi, 3^{11} **mod** $13 = 3$

ALGORITHM 5 Fast Modular Exponentiation.

procedure *modular exponentiation*(b: integer, $n = (a_{k-1}a_{k-2} \ldots a_1a_0)_2$,
m: positive integers)
$x := 1$
$power := b$ **mod** m
for $i := 0$ **to** $k - 1$
  if $a_i = 1$ **then** $x := (x \cdot power)$ **mod** m
  $power := (power \cdot power)$ **mod** m
return $x\{x$ equals b^n **mod** $m\}$

Greatest Common Divisors (GCD)

Faktor Persekutuan terBesar (FPB)

- $\mathrm{GCD}(a, b)$: bilangan terbesar yang membagi habis a dan b, untuk $a \neq 0$ dan $b \neq 0$ adalah bilangan bulat
  - $\mathrm{GCD}(24,36) = 12$
  - $\mathrm{GCD}(17,22) = 1$
- Bilangan bulat a dan b disebut *relatively prime*, jika $\mathrm{GCD}(a, b) = 1$
- Deretan bilangan bulat $a_1, a_2, \ldots a_n$ disebut *pairwise relatively prime* jika $\mathrm{GCD}(a_i, a_j) = 1$, untuk $1 \leq i < j \leq n$.
  - 10, 17, 21 adalah *pairwise relatively prime* karena $\mathrm{GCD}(10,17) = 1$, $\mathrm{GCD}(17,21) = 1$, dan $\mathrm{GCD}(10,21) = 1$
  - 10, 19, 24 bukan *pairwise relatively prime* karena $\mathrm{GCD}(10,24) = 2$

Kongruensi

- $a \equiv b (\mathrm{mod}\ m)$ jika dan hanya jika $a \bmod m = b \bmod m$
  - Contoh: apakah $14 \equiv 8 (\mathrm{mod}\ 6)$?
    - Iya, karena $14 \bmod 6 = 8 \bmod 6$ ➔ $2 = 2$
- Jika m bilangan bulat positif dan a, b, c adalah bilangan bulat. Jika $ac \equiv bc (\mathrm{mod}\ m)$ dan $\mathrm{GCD}(c, m) = 1$, maka $a \equiv b (\mathrm{mod}\ m)$
  - c adalah relatively prime dengan m
  - $m \mid a - b$

Kongruensi Linier (1)

- $ax \equiv b \pmod{m}$, untuk m bilangan bulat positif, a dan b adalah bilangan bulat, dan x adalah peubah.
  - Bagaimana mencari semua nilai x yang memenuhi kongruensi $ax \equiv b \pmod{m}$?
  - **Inverse dari a modulo m**, $\bar{a}a \equiv 1 \pmod{m}$, untuk a dan m adalah *relatively prime*.
    - $\bar{a}$ disebut inverse perkalian
    - Gunakan persamaan euclidean untuk mencari $\mathrm{GCD}(a, m) = 1$, yaitu $m = k \cdot a + 1$, dilanjutkan dengan extended euclidean
- Contoh: tentukan inverse dari 3 modulo 7

  $7 = 2 \cdot 3 + 1$ ➔ $-2 \cdot 3 + 1 \cdot 7 = 1$

  maka -2 adalah inverse dari 3 modulo 7

  Selain itu, $(-2 + 7) = 5$ dan 12 juga termasuk dari inverse dari 3 modulo 7

Kongruensi Linier (2)

- Solusi untuk $3x \equiv 4 (\mathrm{mod}\ 7)$

  Inverse dari 3 modulo 7 adalah -2

  $-2 \cdot 3 = -6 \equiv 1 (\mathrm{mod}\ 7)$

  $-2 \cdot 3x \equiv -2 \cdot 4 (\mathrm{mod}\ 7)$

  $x \equiv -8 (\mathrm{mod}\ 7)$

  $x \bmod 7 = -8 \bmod 7$

  $x \bmod 7 = 6$

  $x \equiv 6 (\mathrm{mod}\ 7)$

  Untuk $x = 6$, maka $3 \cdot 6 = 18 \equiv 4 (\mathrm{mod}\ 7)$

  Solusi lainnya untuk x adalah $6 + 7 = 13, 20, \ldots$ dan $-1, -8, -15, \ldots$

https://www.math.uh.edu/~pwalker/3336Sp21Sec4.4Slides.pdf

Contoh Inverse a Modulo m

- Inverse 55 modulo 7

  Euclidean:

  $55 = 7 \cdot 7 + 6$ ➔ $6 = 55 - 7 \cdot 7$

  $7 = 1 \cdot 6 + 1$ ➔ $1 = 7 - 1 \cdot 6$

  Extended Euclidean:

  $1 = 7 - 1 \cdot (55 - 7 \cdot 7)$

  $1 = 8 \cdot 7 - 1 \cdot 55$

  Inverse 55 modulo $7 = -1$,

  atau nilai positifnya $(-1 + 7) = 6$

  Inverse 55 modulo $7 = 6$

- Inverse 7 modulo 31

  Euclidean:

  $31 = 4 \cdot 7 + 3$ ➔ $3 = 31 - 4 \cdot 7$

  $7 = 2 \cdot 3 + 1$ ➔ $1 = 7 - 2 \cdot 3$

  Extended Euclidean:

  $1 = 7 - 2 \cdot (31 - 4 \cdot 7)$

  $1 = 9 \cdot 7 - 2 \cdot 31$

  Inverse 7 modulo $31 = 9$

Teori Bilangan untuk Kriptografi

Teori Bilangan dan Kriptografi

- Teori bilangan berperan penting untuk kriptografi
  - Proses merubah (**enkripsi**) informasi asli (*plaintext*), menggunakan sebuah atau lebih kunci, menjadi informasi yang sulit dimengerti atau bisa dibaca oleh pihak lain (*ciphertext*).
  - Proses mengembalikan (dekripsi) *ciphertext* ke *plaintext* dengan kunci rahasia yang sama atau berbeda.
- Jenis kriptografi ditentukan dari kunci yang digunakan.
  - Simetris: kunci rahasia yang digunakan untuk enkripsi dan dekripsi sama
  - Asimetris: kunci rahasia yang digunakan untuk enkripsi dan dekripsi berbeda

Model Enkripsi Simetris

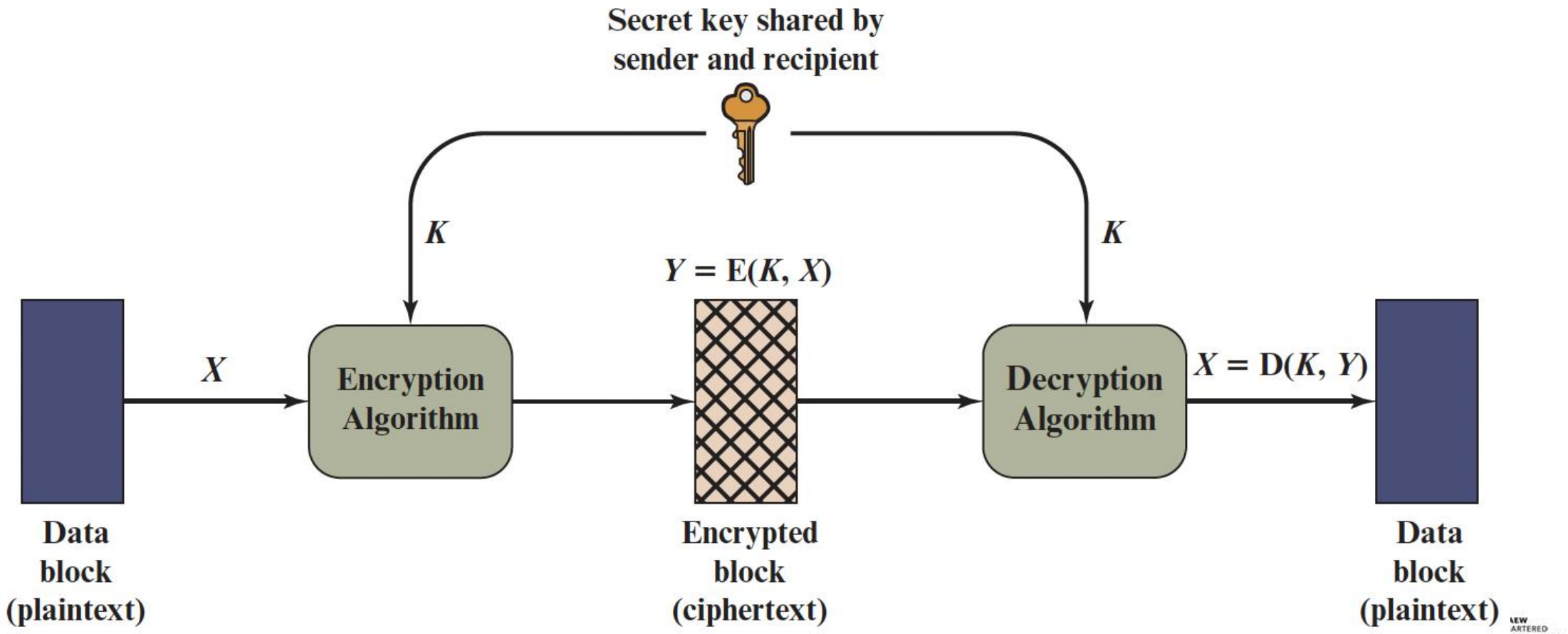


Figure 3.1 Simplified Model of Symmetric Encryption

Table konversi dari huruf ke angka:

A atau a = 0	K atau k = 10	U atau u = 20
B atau b = 1	L atau l = 11	V atau v = 21
C atau c = 2	M atau m = 12	W atau w = 22
D atau d = 3	N atau n = 13	X atau x = 23
E atau e = 4	O atau o = 14	Y atau y = 24
F atau f = 5	P atau p = 15	Z atau z = 25
G atau g = 6	Q atau q = 16	
H atau h = 7	R atau r = 17	
I atau i = 8	S atau s = 18	
J atau j = 9	T atau t = 19	

Kriptografi Simetris – Klasik (1)

- Shift Ciphers: mempertukarkan karakter
  - Caesar cipher:
    - Enkripsi: $c = (p + k) \bmod 26$
    - Dekripsi: $p = (c - k) \bmod 26$
    - $p =$ karakter pada plaintext
    - $c =$ karakter pada ciphertext
    - $k =$ bilangan (kunci rahasia)
  - Affine cipher:
    - Enkripsi: $c = (ap + b) \bmod 26$
    - Dekripsi: $p \equiv \bar{a}(c - b) \pmod{26}$
    - $a =$ kunci rahasia pertama
    - $\bar{a} =$ inverse dari a
    - $b =$ kunci rahasia kedua

- Cara menentukan formula dekripsi Affine cipher:
  - $c \equiv (ap + b) \pmod{26}$
  - $c - b \equiv ap \pmod{26}$
  - karena $\mathrm{GCD}(a, 26) = 1$, maka terdapat inverse $\bar{a}$ dari a module 26
  - $\bar{a}\,(c - b) \equiv \bar{a}ap \pmod{26}$, karena $\bar{a}a = 1$
  - $p \equiv \bar{a}(c - b) \pmod{26}$

Kriptografi Simetris – Klasik (2)

- Block Ciphers: transposition cipher
  - Menggunakan kunci permutasi σ untuk himpunan $\{1,2, \dots, m\}$, untuk m adalah bilangan bulat positif, yang dipetakan *one-to-one* ke himpunan $\{1,2, \dots, m\}$ juga.
  - Enkripsi: $c_1 c_2 \dots c_m = p_{\sigma(1)} p_{\sigma(2)} \cdots p_{\sigma(m)}$
  - Dekripsi: $p_1 p_2 \dots p_m = p_{\sigma^{-1}(1)} p_{\sigma^{-1}(2)} \cdots p_{\sigma^{-1}(m)}$
  - Kunci untuk enkripsi $\sigma(i) = j$, karakter ke-i dipindahkan ke posisi j
  - Kunci untuk dekripsi $\sigma^{-1}(j) = i$, karakter ke-j dipindahkan ke posisi i

A atau a = 0	K atau k = 10	U atau u = 20
B atau b = 1	L atau l = 11	V atau v = 21
C atau c = 2	M atau m = 12	W atau w = 22
D atau d = 3	N atau n = 13	X atau x = 23
E atau e = 4	O atau o = 14	Y atau y = 24
F atau f = 5	P atau p = 15	Z atau z = 25
G atau g = 6	Q atau q = 16	
H atau h = 7	R atau r = 17	
I atau i = 8	S atau s = 18	
J atau j = 9	T atau t = 19	

- $c = (13 + 3) \bmod 26 = 16$
- $c = (14 + 3) \bmod 26 = 17$
- $c = (22 + 3) \bmod 26 = 25$
- Ciphertext = UXQ QRZ

Caesar Cipher

- Dekripsi: $p = (c - k) \bmod 26$
  - $p = (20 - 3) \bmod 26 = 17$
  - $p = (23 - 3) \bmod 26 = 20$
  - $p = (16 - 3) \bmod 26 = 13$
  - $p = (16 - 3) \bmod 26 = 13$
  - $p = (17 - 3) \bmod 26 = 14$
  - $p = (25 - 3) \bmod 26 = 22$
  - *Plaintext*: RUN NOW

Contoh Perhitungan Affine Cipher

A atau a = 0	K atau k = 10	U atau u = 20
B atau b = 1	L atau l = 11	V atau v = 21
C atau c = 2	M atau m = 12	W atau w = 22
D atau d = 3	N atau n = 13	X atau x = 23
E atau e = 4	O atau o = 14	Y atau y = 24
F atau f = 5	P atau p = 15	Z atau z = 25
G atau g = 6	Q atau q = 16	
H atau h = 7	R atau r = 17	
I atau i = 8	S atau s = 18	
J atau j = 9	T atau t = 19	

- Dekripsi: $p \equiv \bar{a}(c - b)\ (\mathbf{mod}\ 26)$
- Gunakan extended Euclidean untuk mendapatkan inverse $\bar{a}$
- $\bar{a} = 9$
- $p \equiv 9\ (c - 8)(\mathbf{mod}\ 26)$
- $p = 9\ (c - 8)\mathbf{mod}\ 26$
  - $p = 9\ (7 - 8)\mathbf{mod}\ 26 = 17$
  - $p = 9\ (16 - 8)\mathbf{mod}\ 26 = 20$
  - $p = 9\ (21 - 8)\mathbf{mod}\ 26 = 13$
  - $p = 9\ (21 - 8)\mathbf{mod}\ 26 = 13$
  - $p = 9\ (24 - 8)\mathbf{mod}\ 26 = 14$
  - $p = 9\ (22 - 8)\mathbf{mod}\ 26 = 22$
  - *Plaintext*: RUN NOW

Contoh Perhitungan Transposition Cipher

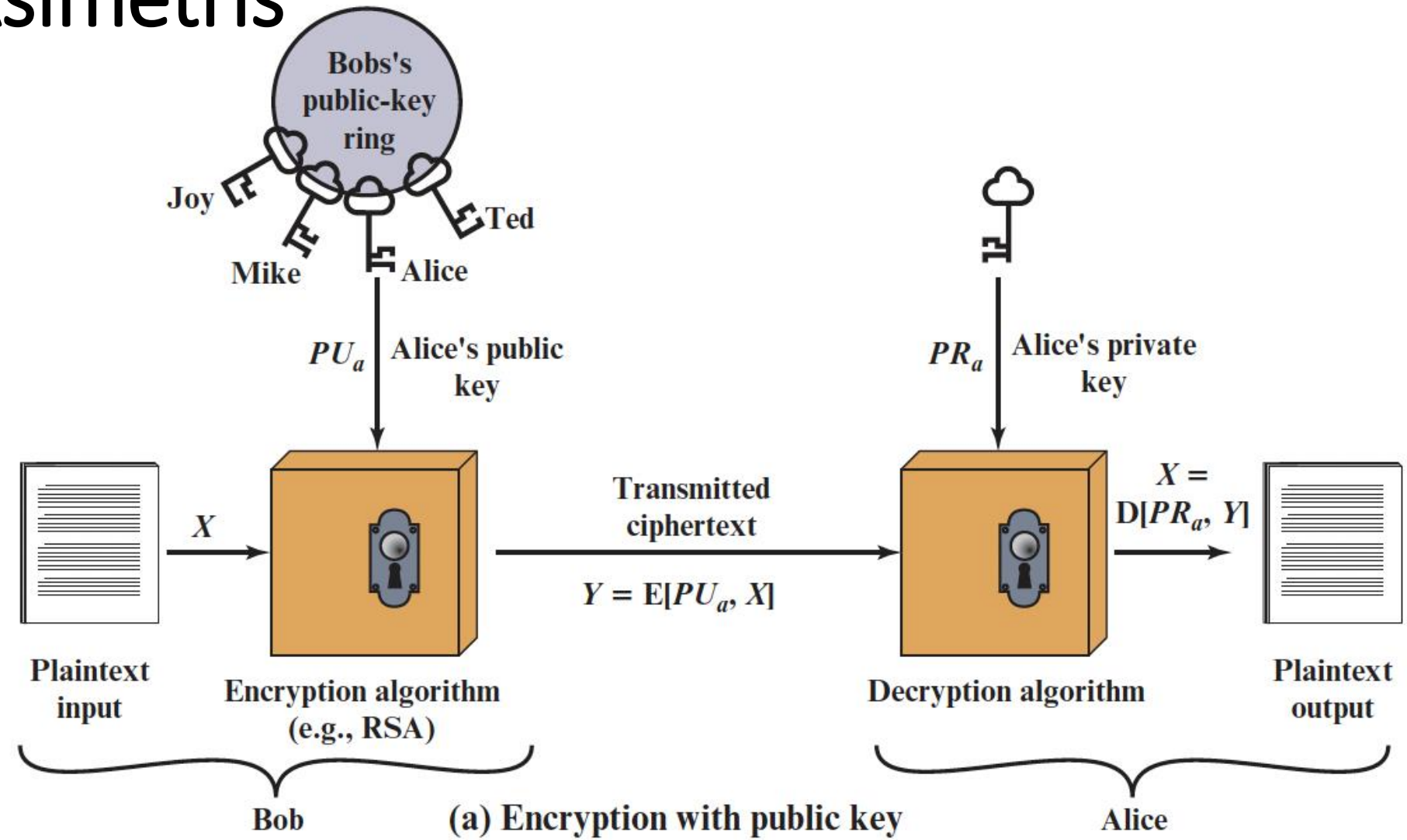
- *Plaintext*: “RUN NOW”
- Kunci rahasia $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$
- Enkripsi:
  - Ciphertext = NRU WNO

N	R	U

W	N	O

- Dekripsi:
  - Kunci rahasia $\sigma^{-1}(2) = 1, \sigma^{-1}(3) = 2, \sigma^{-1}(1) = 3$
  - *Plaintext*: RUN NOW

Kriptografi
Kunci Asimetris



Kriptografi Kunci Asimetris

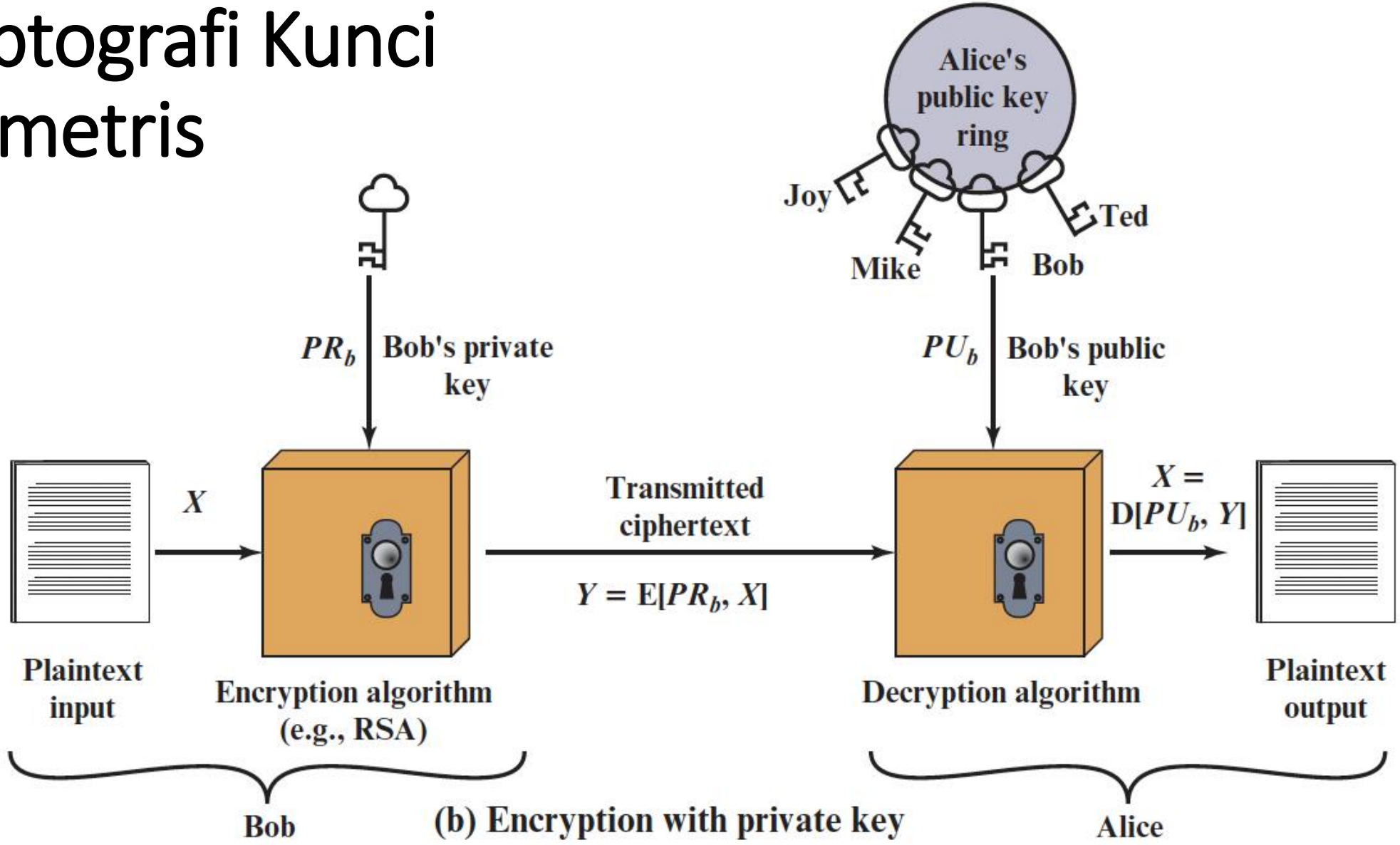


Figure 9.1 Public-Key Cryptography

Kriptografi Asimetris Rivest–Shamir-Adleman (RSA)

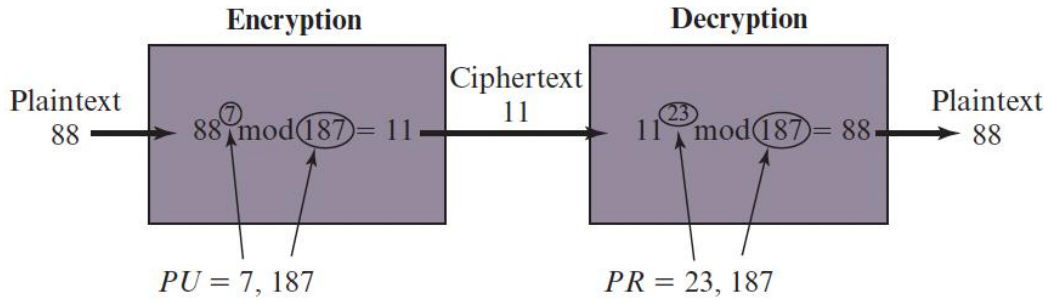
- Baca Buku Kenneth H. Rosen dkk halaman 315 – 320

Key Generation by Alice	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n)=(p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Private Key	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Figure 9.5 The RSA Algorithm



Kriptografi dengan Matriks dan Inverse-nya

Kriptografi dengan matriks $\boldsymbol{A}$ dan Inversnya Hill Cipher

Diketahui pesan yang akan di-encoding (di-enkripsi):

1. Konversikan pesan ke nilai numeriknya
   - Tabel konversi
2. Tentukan matriks kuadrat A berukuran $n \times n$ dan hitung invers A^{-1}
3. Kelompokkan pesan menjadi sejumlah vektor $P = \{\mathbf{p_1}, \mathbf{p_2}, \dots\}$
   - setiap vektor $\mathbf{p_i}$ berukuran $n \times 1$
   - Lakukan padding (misalnya spasi) jika diperlukan
4. Untuk encryption, hitung $\mathbf{c_i} = (A \times \mathbf{p_i}) \mathbf{mod}\ 26$
5. Untuk decryption, hitung $\mathbf{p_i} = (A^{-1} \times \mathbf{c_i}) \mathbf{mod}\ 26$
   - vektor $\mathbf{c_i}$ adalah ciphertext berukuran $n \times 1$

Contoh:

Diketahui sebuah pesan “Run NOW”

1. “Run” = 17 20 13
2. Matriks $A = \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix}$, $A^{-1} = \begin{bmatrix} 1 & 2 & -1 \\ -1 & -3 & 2 \\ -1 & -1 & 1 \end{bmatrix}$
3. $\mathbf{p_1} = \begin{bmatrix} 17 \\ 20 \\ 13 \end{bmatrix}$
4. Encryption : $\mathbf{c_1} = A \times \mathbf{p_1} = \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 17 \\ 20 \\ 13 \end{bmatrix} = \begin{bmatrix} 24 \\ 30 \\ 67 \end{bmatrix} \mathbf{mod}\ 26 = \begin{bmatrix} 24 \\ 4 \\ 15 \end{bmatrix} \Longrightarrow$ YEP
5. Decryption: $\mathbf{p_1} = A^{-1} \times \mathbf{c_1} = \begin{bmatrix} 1 & 2 & -1 \\ -1 & -3 & 2 \\ -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 24 \\ 4 \\ 15 \end{bmatrix} \mathbf{mod}\ 26 = \begin{bmatrix} 17 \\ 20 \\ 13 \end{bmatrix}$

Contoh:

Diketahui sebuah pesan “Run NOW”

1. “NOW” = 13 14 22

2. Matriks $A = \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix}$, $A^{-1} = \begin{bmatrix} 1 & 2 & -1 \\ -1 & -3 & 2 \\ -1 & -1 & 1 \end{bmatrix}$

3. $\mathbf{p_2} = \begin{bmatrix} 13 \\ 14 \\ 22 \end{bmatrix}$

4. Encryption : $\mathbf{c_2} = A \times \mathbf{p_2} = \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 13 \\ 14 \\ 22 \end{bmatrix} = \begin{bmatrix} 5 \\ 35 \\ 42 \end{bmatrix} \mathbf{mod}\ 26 = \begin{bmatrix} 5 \\ 9 \\ 10 \end{bmatrix} \Longrightarrow$ FJK

5. Decryption: $\mathbf{p_2} = A^{-1} \times \mathbf{c_2} = \begin{bmatrix} 1 & 2 & -1 \\ -1 & -3 & 2 \\ -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 5 \\ 9 \\ 10 \end{bmatrix} \mathbf{mod}\ 26 = \begin{bmatrix} 13 \\ 14 \\ 22 \end{bmatrix}$

A atau a = 0	K atau k =
B atau b = 1	L atau l =
C atau c = 2	M atau m
D atau d = 3	N atau n =
E atau e = 4	O atau o =
F atau f = 5	P atau p =
G atau g = 6	Q atau q =
H atau h = 7	R atau r =
I atau i = 8	S atau s =
J atau j = 9	T atau t =

Latihan Soal

Diketahui pesan “DO NOT WALK DOG”. Gunakan kriptografi berikut untuk merubah pesan (enkripsi) dan mengembalikannya kembali (dekripsi). Ingat, jawaban harus disertakan proses perhitungan!

1. Caesar Cipher dengan $k = 17$
2. Affine Cipher dengan $a = 17$ dan $b = 5$
3. Transposition Cipher dengan $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 4$ dan $\sigma(4) = 2$
4. Kriptografi dengan kunci rahasia adalah $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix}$