ALGORITMA DAN BILANGAN BULAT (INTEGER)

IK-130
LOGIKA INFORMATIKA

Ani Anisyah, M.T.

IK130 - Logika Informatika

OUTLINE

- **Definisi Bilangan Bulat (Integer)**
- **Sifat-sifat bilangan bulat**
- **Algoritma Euclid**
- **PBT**
- **Relatif Prima**
- **Aritmatika Modulo**
- **Kongruen**
- Balikan Modulo
- Bilangan Prima
- Implementasi Bilangan Bulat
  - ISBN
  - Fungsi Hash
  - Kriptografi (Inskripsi Deskripsi, Algoritma RSA)
  - Pembangkit bilangan acak-semu

DEFINISI BILANGAN BULAT

- **Bilangan bulat** adalah bilangan yang **tidak mempunyai pecahan desimal**, misalnya 8, 21, 8765, -34, 0

- Berlawanan dengan bilangan bulat adalah **bilangan riil** yang **mempunyai titik desimal**, seperti 8.0, 34.25, 0.02.

SIFAT PEMBAGIAN PADA BILANGAN BULAT

- Misalkan a dan b bilangan bulat, $a \neq 0$.

  a **habis membagi** b (*a divides b*) jika terdapat bilangan bulat c sedemikian sehingga $b = ac$.

- Notasi: $a \mid b$ jika $b = ac$, $c \in$ **Z** dan $a \neq 0$.

- **Contoh 1**: $4 \mid 12$ karena $12/4 = 3$ (bilangan bulat) atau $12 = 4 \times 3$. Tetapi $4 \mid 13$ karena $13/4 = 3.25$ (bukan bilangan bulat).

Teorema Euclidean

- **Teorema 1 (Teorema Euclidean).** Misalkan *m* dan *n* bilangan bulat, $n > 0$. Jika *m* dibagi dengan *n* maka terdapat bilangan bulat unik *q* (*quotient*) dan *r* (*remainder*), sedemikian sehingga.

$$m = nq + r$$

10 : 2 = 5 sisa 0
10 : 3 = 3 sisa 1

Contoh : 10 : 3
m = nq + r
10 = 3.3 + 1

dengan $0 \leq r < n$.

Contoh:

$m = nq + r$

Contoh 2.

(i) 1987/97 = 20, sisa 47:

$1987 = 97 \cdot 20 + 47$

(ii) –22/3 = –8, sisa 2:

$-22 = 3(-8) + 2$

- tetapi jika pembagiannya sebagai berikut:

$-22 = 3(-7)$ sisa -1

$-22 = (-7) \cdot 3 - 1$ (salah)

karena $r = -1$ (syarat $0 \leq r < n$)

Pembagian Bersama Terbesar (PBB)

- Misalkan *a* dan *b* bilangan bulat tidak nol.

- Pembagi bersama terbesar (PBB – **greatest common divisor** atau *gcd*) dari *a* dan *b* adalah bilangan bulat terbesar *d* sedemikian hingga $d \mid a$ dan $d \mid b$.

- Dalam hal ini kita nyatakan bahwa PBB(*a*, *b*) = *d*.

Contoh:

- Faktor pembagi 45: 1, 3, 5, 9, 15, 45;
- Faktor pembagi 36: 1, 2, 3, 4, 9, 12, 18, 36;
- Faktor pembagi bersama 45 dan 36: 1, 3, 9

→ PBB(45, 36) = 9.

- **Teorema 2.** Misalkan m dan n bilangan bulat, dengan syarat $n > 0$ sedemikian sehingga

$$m = nq + r \quad , 0 \leq r < n$$

maka PBB(m, n) = PBB(n, r)

- **Contoh 4**: $m = 60$, $n = 18$,

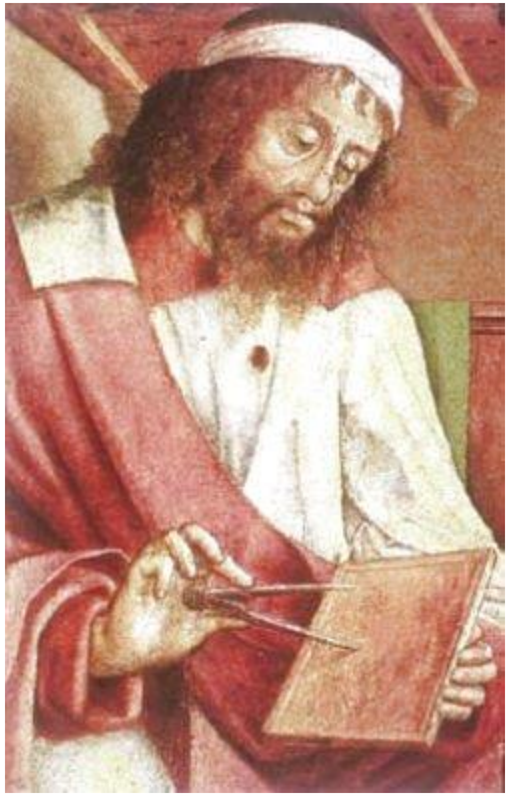
$$60 = 18 \cdot 3 + 6$$

maka PBB(60, 18) = PBB(18, 6) = 6

Algoritma Euclidean

- Tujuan: algoritma untuk mencari PBB dari dua buah bilangan bulat.

- Penemu: Euclides, seorang matematikawan Yunani yang menuliskan algoritmanya tersebut dalam buku, *Element*.



Misalkan m dan n adalah bilangan bulat tak negatif dengan $m \geq n$.
Misalkan $r_0 = m$ dan $r_1 = n$.
Lakukan secara berturut-turut pembagian untuk memperoleh

$$r_0 = r_1 q_1 + r_2 \qquad 0 \leq r_2 \leq r_1,$$
$$r_1 = r_2 q_2 + r_3 \qquad 0 \leq r_3 \leq r_2,$$

$$r_{n-2} = r_{n-1}\, q_{n-1} + r_n \qquad 0 \leq r_n \leq r_{n-1},$$
$$r_{n-1} = r_n q_n + 0$$

Teorema 2. Misalkan m dan n bilangan bulat, dengan syarat $n > 0$ sedemikian sehingga

$$\boldsymbol{m = nq + r \quad , 0 \leq r < n}$$

maka PBB(m, n) = PBB(n, r)

Menurut Teorema 2,

PBB(m, n) = PBB(r_0, r_1) = PBB(r_1, r_2) = … =
PBB(r_{n-2}, r_{n-1}) = PBB(r_{n-1}, r_n) = PBB(r_n, 0) = r_n

Jadi, **PBB dari *m* dan *n*** adalah **sisa terakhir yang tidak nol** dari runtunan pembagian tersebut

Diberikan dua buah bilangan bulat tak-negatif m dan n ($m \geq n$).
Algoritma Euclidean berikut mencari pembagi bersama terbesar dari m dan n.

Algoritma Euclidean

1. Jika $n = 0$ maka
   m adalah PBB(m, n);
   stop.

   tetapi jika $n \neq 0$,
   lanjutkan ke langkah 2.
2. Bagilah m dengan n dan misalkan r adalah sisanya.
3. Ganti nilai m dengan nilai n dan nilai n dengan nilai r, lalu ulang kembali ke langkah 1.

```
procedure Euclidean(input m, n : integer,  output PBB : integer)
{ Mencari PBB(m, n) dengan syarat m dan n bilangan tak-negatif dan m ≥
  n
  Masukan: m dan n, m ≥ n dan m, n ≥ 0
  Keluaran: PBB(m, n)
}
Kamus
   r : integer

Algoritma:
   while n ≠ 0 do
      r ← m mod n
      m ← n
      n ← r
   endwhile
   { n = 0, maka PBB(m,n) = m }
   PBB ← m
```

Contoh 4. $m = 80$, $n = 12$ dan dipenuhi syarat $m \geq n$

$$80 = 6 \cdot 12 + 8$$

$$12 = 1 \cdot 8 + 4$$

$$8 = 2 \cdot 4 + 0$$

Sisa pembagian terakhir sebelum 0 adalah 4, maka PBB(80, 12) = 4.

Kombinasi Lanjar

- PBB(a,b) dapat dinyatakan sebagai **kombinasi lanjar** (*linear combination*) a dan b dengan dengan koefisien-koefisennya.

- **Contoh 6**: PBB(80, 12) = 4 ,

  $$4 = (-1) \cdot 80 + 7 \cdot 12.$$

- **Teorema 3.** Misalkan a dan b bilangan bulat positif, maka terdapat bilangan bulat m dan n sedemikian sehingga PBB(a, b) = $ma + nb$.

Kombinasi Lanjar

- **Contoh 7**: Nyatakan PBB(21, 45) sebagai kombinasi lanjar dari 21 dan 45.
- Solusi:

$$45 = 2\,(21) + 3$$

$$21 = 7\,(3) + 0$$

Sisa pembagian terakhir sebelum 0 adalah 3, maka **PBB(45, 21) = 3**

Substitusi dengan persamaan–persamaan di atas menghasilkan:

$$3 = 1\,.\,45 + (-2).21$$

$$\mathbf{3 = 45 - 2\,(21)}$$

yang merupakan kombinasi lanjar dari 45 dan 21

Kombinasi Lanjar

Contoh 8: Nyatakan PBB(312, 70) sebagai kombinasi lanjar 312 dan 70.

<u>Solusi</u>: Terapkan algoritma Euclidean untuk memperoleh PBB(312, 70):

$312 = 4 \cdot 70 + 32$ (i)

$70 = 2 \cdot 32 + 6$ (ii)

$32 = 5 \cdot 6 + 2$ (iii)

$6 = 3 \cdot 2 + 0$ (iv)

Sisa pembagian terakhir sebelum 0 adalah 2, maka **PBB(312, 70) = 2**

Susun pembagian nomor (iii) dan (ii) masing-masing menjadi

$2 = 32 – 5 \cdot 6$ (iv)

$6 = 70 – 2 \cdot 32$ (v)

Sulihkan (v) ke dalam (iv) menjadi

$2 = 32 – 5\cdot(70 – 2\cdot32) = 1\cdot32 – 5\cdot70 + 10\cdot32 = 11 \cdot 32 – 5 \cdot 70$ (vi)

Susun pembagian nomor (i) menjadi

$32 = 312 – 4 \cdot 70$ (vii)

Sulihkan (vii) ke dalam (vi) menjadi

$2 = 11 \cdot 32 – 5 \cdot 70 = 11 \cdot (312 – 4 \cdot 70) – 5 \cdot 70 = 11 . 312 – 49 \cdot 70$

Jadi, PBB(312, 70) = $2 = 11 \cdot 312 – 49 \cdot 70$

Relatif Prima

- Dua buah bilangan bulat a dan b dikatakan *relatif prima* jika PBB(a, b) = 1.

- **Contoh 9.**

  (i) 20 dan 3 relatif prima sebab PBB(20, 3) = 1.

  (ii) 7 dan 11 relatif prima karena PBB(7, 11) = 1.

  (iii) 20 dan 5 tidak relatif prima sebab PBB(20, 5) = 5 $\neq$ 1.

- Jika a dan b relatif prima, maka terdapat bilangan bulat m dan n sedemikian sehingga

$$ma + nb = 1$$

- **Contoh 10.** Bilangan 20 dan 3 adalah relatif prima karena PBB(20, 3) =1, atau dapat ditulis

$$2 \,.\, 20 + (–13) \,.\, 3 = 1 \quad (m = 2, n = –13)$$

Tetapi 20 dan 5 tidak relatif prima karena PBB(20, 5) = 5 $\neq$ 1 sehingga 20 dan 5 tidak dapat dinyatakan dalam $m \,.\, 20 + n \,.\, 5 = 1$.

Aritmetika Modulo

- Misalkan a dan m bilangan bulat ($m > 0$). Operasi

  a* mod *m (dibaca "*a* modulo *m*")

  memberikan sisa jika a dibagi dengan m.

- Notasi: $a \bmod m = r$ sedemikian sehingga

  $a = mq + r$, dengan $0 \le r < m$.

- m disebut **modulus** atau **modulo**, dan hasil aritmetika modulo m terletak di dalam himpunan $\{0, 1, 2, \ldots, m - 1\}$.

Aritmetika Modulo

- **Contoh 11.** Beberapa hasil operasi dengan operator modulo:

(i) 23 mod 5 = 3	$(23 = 5 \cdot 4 + 3)$
(ii) 27 mod 3 = 0	$(27 = 3 \cdot 9 + 0)$
(iii) 6 mod 8 = 6	$(6 = 8 \cdot 0 + 6)$
(iv) 0 mod 12 = 0	$(0 = 12 \cdot 0 + 0)$
(v) – 41 mod 9 = 4	$(-41 = 9 (-5) + 4)$
(vi) – 39 mod 13 = 0	$(-39 = 13(-3) + 0)$

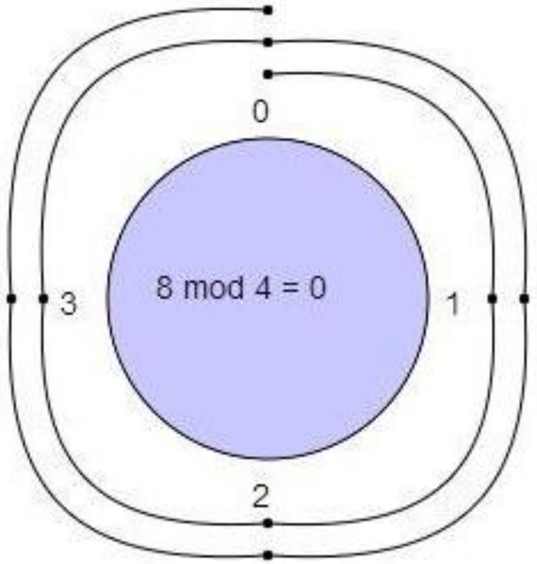
- *Penjelasan untuk (v):* Karena *a* negatif, bagi $|a|$ dengan *m* mendapatkan sisa *r'*. Maka *a* mod *m* = *m* – *r'* bila $r' \neq 0$. Jadi $|-41|$ mod 9 = 5, sehingga –41 mod 9 = 9 – 5 = 4.

Aritmetika Modulo

8 mod 4 = ?

With a modulus of 4 we make a clock with numbers 0,1,2,3

We start at 0 and go through 8 numbers in a clockwise sequence 1,2,3,0,1,2,3,0



Sumber: www.khancademy.org

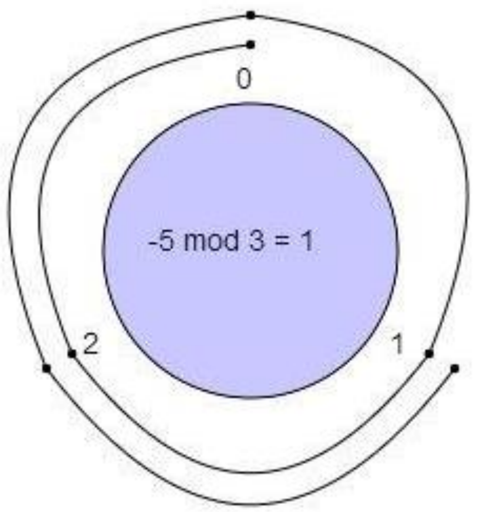
Aritmetika Modulo

-5 mod 3 = ?

With a modulus of 3 we we make a clock with numbers 0,1,2

We start at 0 and go through 5 numbers in **counter-clockwise** sequence (5 is **negative**)

2,1,0,2,1



Sumber: www.khancademy.org

Kongruen

- Misalnya 38 mod 5 = 3 dan 13 mod 5 = 3, maka dikatakan $38 \equiv 13 \pmod 5$ (baca: 38 kongruen dengan 13 dalam modulo 5).

- Misalkan *a* dan *b* bilangan bulat dan *m* adalah bilangan > 0, maka $\boldsymbol{a \equiv b \pmod m}$ jika dan hanya jika $m \mid (a - b)$.

- Jika *a* tidak kongruen dengan *b* dalam modulus *m*, maka ditulis $a \not\equiv b \pmod m$.

- **Contoh 12.**

Misalkan a dan b bilangan bulat dan m adalah bilangan > 0, maka $\boldsymbol{a \equiv b \pmod{m}}$ jika dan hanya jika $m \mid (a - b)$.

$17 \equiv 2 \pmod 3$ *(3 habis membagi 17 – 2 = 15 → 15 : 3 = 5)*

$-7 \equiv 15 \pmod{11}$

(11 habis membagi –7 – 15 = –22 → -22 : 11 = 2)

$12 \not\equiv 2 \pmod 7$

(7 tidak habis membagi 12 – 2 = 10)

$-7 \not\equiv 15 \pmod 3$

(3 tidak habis membagi –7 – 15 = –22)

Latihan

Definisi Kongruen: Misalkan a dan b bilangan bulat dan m adalah bilangan > 0, maka $\boldsymbol{a \equiv b}$ **(mod $\boldsymbol{m}$)** jika dan hanya jika $m \mid (a - b)$.

- Tentukan semua bilangan yang kongruen dengan 5 (mod 11).

- <u>Penyelesaian</u>: Misalkan bilangan yang kongruen dengan 5 (mod 11) adalah x.

  $x \equiv 5 \pmod{11}$

  Jadi, $11 \mid (x - 5)$, atau $\frac{x-5}{11}$ = bilangan bulat

- Nilai x yang memenuhi adalah 16, 27, 38, ..., lalu -6, -17, ...

- Jadi, nilai-nilai yang kongruen dengan 5 (mod 11) adalah ..., -17, –6, 16, 27, 38, ...

Latihan

Definisi Kongruen: Misalkan *a* dan *b* bilangan bulat dan *m* adalah bilangan > 0, maka ***a* ≡ *b* (mod *m*)** jika dan hanya jika *m* | (*a* – *b*).

- Kekungruenan a ≡ b (mod m) dapat ditulis juga dalam hubungan

  a = b + km

  k → bilangan bulat

- Contoh :
  - 38 ≡ 13 (mod 5) dapat ditulis sebagai 38 = 13 + 5.5 → k = 5
  - 17 ≡ 2 (mod 3) dapat ditulis sebagai 17 = 2 + 5.3 → k = 5
  - -7 ≡ 15 (mod 11) dapat ditulis sebagai -7 = 15 + (-2).11 → k = -2

Teorema 4. Misalkan m adalah bilangan bulat positif.

1)Jika $a \equiv b \pmod{m}$ dan c adalah sembarang bilangan bulat maka

(i) $(a + c) \equiv (b + c) \pmod{m}$

(ii) $ac \equiv bc \pmod{m}$

(iii) $a^p \equiv b^p \pmod{m}$, p bilangan bulat tak-negatif

2) Jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka

(i) $(a + c) \equiv (b + d) \pmod{m}$

(ii) $ac \equiv bd \pmod{m}$

Bukti (hanya untuk 1(ii) dan 2(i) saja):

1(ii) $a \equiv b \pmod{m}$ berarti:

$ac \equiv bc \pmod{m}$

$\Leftrightarrow a = b + km$

$\Leftrightarrow a - b = km$

$\Leftrightarrow (a - b)c = ckm$

$\Leftrightarrow ac = bc + Km$

$\Leftrightarrow ac \equiv bc \pmod{m}$

2(i) $a \equiv b \pmod{m} \Leftrightarrow a = b + k_1 m$

$(a + c) \equiv (b + c) \pmod{m}$

$c \equiv d \pmod{m} \Leftrightarrow c = d + k_2 m \;\; +$

$\Leftrightarrow (a + c) = (b + d) + (k_1 + k_2)m$

$\Leftrightarrow (a + c) = (b + d) + km \; (k = k_1 + k_2)$

$\Leftrightarrow (a + c) = (b + d) \pmod{m}$

Latihan

Contoh 15.

Misalkan $17 \equiv 2 \pmod 3$ dan $10 \equiv 4 \pmod 3$, maka menurut Teorema 4,

$17 + 5 = 2 + 5 \pmod 3$ $\Leftrightarrow$ $22 = 7 \pmod 3$ (Teorema 4.i)

$17 . 5 = 5 \cdot 2 \pmod 3$ $\Leftrightarrow$ $85 = 10 \pmod 3$ (Teorema 4.ii)

$17 + 10 = 2 + 4 \pmod 3$ $\Leftrightarrow$ $27 = 6 \pmod 3$ (Teorema 4.i)

$17 . 10 = 2 \cdot 4 \pmod 3$ $\Leftrightarrow$ $170 = 8 \pmod 3$ (Teorema 4.ii)

Latihan

Contoh 15.

Misalkan $17 \equiv 2 \pmod{3}$ dan $10 \equiv 4 \pmod{3}$, maka menurut Teorema 4,

$17 + 5 = 2 + 5 \pmod{3} \Leftrightarrow 22 = 7 \pmod{3}$

$17 . 5 = 5 \cdot 2 \pmod{3} \Leftrightarrow 85 = 10 \pmod{3}$

$17 + 10 = 2 + 4 \pmod{3} \Leftrightarrow 27 = 6 \pmod{3}$

$17 . 10 = 2 \cdot 4 \pmod{3} \Leftrightarrow 170 = 8 \pmod{3}$

Latihan

- Teorema 4 tidak memasukkan operasi pembagian pada aritmetika modulo karena jika kedua ruas dibagi dengan bilangan bulat, maka kekongruenan tidak selalu dipenuhi.

- **Contoh 16**:

  $10 \equiv 4 \pmod 3$ dapat dibagi dengan 2

  karena $10/2 = 5$ dan $4/2 = 2$, dan $5 \equiv 2 \pmod 3$

  $14 \equiv 8 \pmod 6$ tidak dapat dibagi dengan 2, karena $14/2 = 7$ dan $8/2 = 4$, tetapi $7 \not\equiv 4 \pmod 6$.

Latihan

Jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$ adalah sembarang bilangan bulat maka buktikan bahwa

$$ac \equiv bd \pmod{m}$$

Solusi

$a \equiv b \pmod{m} \rightarrow a = b + k_1 m$

$c \equiv d \pmod{m} \rightarrow c = d + k_2 m$

maka

$\Leftrightarrow ac = (b + k_1 m)(d + k_2 m)$

$\Leftrightarrow ac = bd + bk_2 m + dk_1 m + k_1 k_2 m^2$

$\Leftrightarrow ac = bd + Km$ dengan $K = bk_2 + dk_1 + k_1 k_2 m$

$\Leftrightarrow$ $\boldsymbol{ac \equiv bd \pmod{m}}$ (terbukti)

Tugas

- Cari dan pelajari tentang Implementasi/Penerapan Bilangan Bulat pada:
  - ISBN
  - Fungsi Hash
  - Kriptografi
  - Algoritma RSA
- Sumber yang dapat digunakan adalah : jurnal, buku, sumber-sumber yang ada di internet
- Dibuat dalam bentuk file .pdf dan tuliskan sumber
- Setiap pembahasan minimal dibahas oleh 2 kelompok (3 kelompok jika jumlah kelompok di kelas berjumlah ganjil)

Balikan Modulo (*Modulo Invers*)

- Di dalam aritmetika bilangan riil, balikan atau inversi (*inverse*) dari perkalian adalah pembagian.
- Contoh: Balikan 4 adalah 1/4, sebab $4 \times 1/4 = 1$.
- Di dalam aritmetika modulo, masalah menghitung balikan modulo lebih sukar.

Balikan Modulo (*Modulo Invers*)

- **Syarat**: Jika a dan m relatif prima dan $m > 1$, maka balikan (*invers*) dari a (mod m) ada.

- Balikan dari a (mod m) adalah bilangan bulat x sedemikian sehingga:

$$xa \equiv 1 \pmod{m}$$

- Dalam notasi lainnya, $a^{-1} \pmod{m} = x$

Balikan Modulo (*Modulo Invers*)

Bukti: a dan m relatif prima, jadi PBB(a, m) = 1, dan terdapat bilangan bulat x dan y sedemikian sehingga:

$$xa + ym = 1$$

yang mengimplikasikan bahwa

$$xa + ym \equiv 1 \pmod{m}$$

Karena $ym \equiv 0 \pmod{m}$ (kenapa?), maka

$$xa \equiv 1 \pmod{m}$$

Kekongruenan yang terakhir ini berarti bahwa x adalah balikan dari a (mod m).

Balikan Modulo (*Modulo Invers*)

- Pembuktian di atas juga menceritakan bahwa untuk mencari balikan dari *a* (mod *m*), kita harus membuat kombinasi lanjar dari *a* dan *m* sama dengan 1.

- Koefisien *a* dari kombinasi lanjar tersebut merupakan balikan dari *a* (mod *m*).

Contoh 17. Tentukan balikan dari 4 (mod 9), 17 (mod 7), dan 18 (mod 10).

Penyelesaian:

(a) Karena PBB(4, 9) = 1, maka balikan dari 4 (mod 9) ada. Dari algoritma Euclidean diperoleh bahwa

$$9 = 2 \cdot 4 + 1$$

Susun persamaan di atas menjadi

$$-2 \cdot 4 + 1 \cdot 9 = 1$$

Dari persamaan terakhir ini kita peroleh –2 adalah balikan dari 4 (mod 9).

Periksa bahwa $-2 \cdot 4 \equiv 1 \pmod{9}$

- Catatan: setiap bilangan yang kongruen dengan

  –2 (**mod** 9)

  juga adalah balikan dari 4, misalnya 7, –11, 16, dan seterusnya, karena

  7 ≡ –2 (**mod** 9) (9 habis membagi 7 – (–2) = 9)

  –11 ≡ –2 (**mod** 9) (9 habis membagi –11 – (–2) = –9)

  16 ≡ –2 (**mod** 9) (9 habis membagi 16 – (–2) = 18)

- (b) Karena PBB(17, 7) = 1, maka balikan dari 17 (mod 7) ada. Dari algoritma Euclidean diperoleh rangkaian pembagian berikut:

$17 = 2 \cdot 7 + 3$ (i)

$7 = 2 \cdot 3 + 1$ (ii)

$3 = 3 \cdot 1 + 0$ (iii) (yang berarti: PBB(17, 7) = 1))

Susun (ii) menjadi:

$1 = 7 - 2 \cdot 3$ (iv)

Susun (i) menjadi

$3 = 17 - 2 \cdot 7$ (v)

Sulihkan (v) ke dalam (iv):

$1 = 7 - 2 \cdot (17 - 2 \cdot 7) = 1 \cdot 7 - 2 \cdot 17 + 4 \cdot 7 = 5 \cdot 7 - 2 \cdot 17$

atau

$-2 \cdot 17 + 5 \cdot 7 = 1$

Dari persamaan terakhir diperoleh –2 adalah balikan dari 17 (mod 7)

$-2 \cdot 17 \equiv 1 \pmod 7$ (7 habis membagi $-2 \cdot 17 - 1 = -35$)

(c) Karena PBB(18, 10) = 2 $\neq$ 1, maka balikan dari 18 (mod 10) tidak ada.

Cara lain menghitung balikan

- Ditanya: balikan dari a (mod m)
- Misalkan x adalah balikan dari a (mod m), maka

  $ax \equiv 1 \pmod{m}$ (definisi balikan modulo)

  atau dalam notasi 'sama dengan':

  $ax = 1 + km$

  atau

  $x = (1 + km)/a$

  Cobakan untuk k = 0, 1, 2, … dan k = -1, -2, …

  Solusinya adalah semua bilangan bulat yang memenuhi.

Cara lain menghitung balikan

- **Contoh 18**: Balikan dari 4 (mod 9) adalah x sedemikian sehingga $4x \equiv 1 \pmod 9$

$4x \equiv 1 \pmod 9 \rightarrow 4x = 1 + 9k \rightarrow x = (1 + 9k)/4$

Untuk $k = 0 \rightarrow x$ tidak bulat

$k = 1 \rightarrow x$ tidak bulat

$k = 2 \rightarrow x$ tidak bulat

$k = 3 \rightarrow x = (1 + 9 \cdot 3)/4 = 7$

$k = -1 \rightarrow x = (1 + 9 \cdot -1)/4 = -2$

Balikan dari 4 (mod 9) adalah 7 (mod 9),

-2 (mod 9), dst

Latihan

- Tentukan semua balikan dari 9 (mod 11).

SOLUSI

- Misalkan 9^{-1} (mod 11) = x
- Maka $9x \equiv 1$ (mod 11) atau $9x = 1 + 11k$ atau

  $x = (1 + 11k)/9$

  Dengan mencoba semua nilai k yang bulat (k = 0, -1, -2, ..., 1, 2, ...) maka
- diperoleh x = 5. Semua bilangan lain yang kongruen dengan 5 (mod 11) juga merupakan solusi, yaitu –6, 16, 27, ...

Kekongruenan Lanjar

- Kekongruenan lanjar berbentuk:

$$ax \equiv b \pmod{m}$$

(m > 0, a dan b sembarang bilangan bulat, dan x adalah peubah bilangan bulat).

Pemecahan: $ax = b + km$ ➔ $x = \frac{b+km}{a}$

(Cobakan untuk k = 0, 1, 2, … dan k = –1, –2, … yang menghasilkan x sebagai bilangan bulat)

Contoh 19.

Tentukan solusi: $4x \equiv 3 \pmod 9$ dan $2x \equiv 3 \pmod 4$

Penyelesaian:

(i) $4x \equiv 3 \pmod 9$

$$x = \frac{3 + k \cdot 9}{4}$$

$k = 0 \rightarrow x = (3 + 0 \cdot 9)/4 = 3/4$ (bukan solusi)

$k = 1 \rightarrow x = (3 + 1 \cdot 9)/4 = 3$

$k = 2 \rightarrow x = (3 + 2 \cdot 9)/4 = 21/4$ (bukan solusi)

$k = 3$, $k = 4$ tidak menghasilkan solusi

$k = 5 \rightarrow x = (3 + 5 \cdot 9)/4 = 12$

…

$k = -1 \rightarrow x = (3 - 1 \cdot 9)/4 = -6/4$ (bukan solusi)

$k = -2 \rightarrow x = (3 - 2 \cdot 9)/4 = -15/4$ (bukan solusi)

$k = -3 \rightarrow x = (3 - 3 \cdot 9)/4 = -6$

…

$k = -6 \rightarrow x = (3 - 6 \cdot 9)/4 = -15$

…

Nilai-nilai x yang memenuhi: 3, 12, … dan –6, –15, …

(ii) $2x \equiv 3 \pmod 4$

$$x = \frac{3 + k \cdot 4}{2}$$

Karena $4k$ genap dan 3 ganjil maka penjumlahannya menghasilkan ganjil, sehingga hasil penjumlahan tersebut jika dibagi dengan 2 tidak menghasilkan bilangan bulat. Dengan kata lain, tidak ada nilai-nilai x yang memenuhi $2x \equiv 3 \pmod 5$.

Cara lain menghitung solusi $ax \equiv b \pmod{m}$

- Seperti dalam persamaan biasa,

  $4x = 12$ → kalikan setiap ruas dengan 1/4 (yaitu invers 4), maka $1/4 \cdot 4x = 12 \cdot 1/4$ → $x = 3$

- $4x \equiv 3 \pmod 9$ → kalikan setiap ruas dengan balikan dari

  4 (mod 9) (dalam hal ini sudah kita hitung, yaitu –2)

  $(-2) \cdot 4x \equiv (-2) \cdot 3 \pmod 9 \Leftrightarrow -8x \equiv -6 \pmod 9$

Karena $-8 \equiv 1 \pmod 9$, maka $x \equiv -6 \pmod 9$. Semua blangan bulat yang kongruen dengan –6 (mod 9) adalah solusinya, yitu 3, 12, …, dan –6, -15, …

Solusi

Misal : bilangan bulat = x

x mod 3 = 2 → $x \equiv 2 \pmod 3$

x mod 5 = 3 → $x \equiv 3 \pmod 5$

Jadi, terdapat sistem kekongruenan:

$x \equiv 2 \pmod 3$ (i)

$x \equiv 3 \pmod 5$ (ii)

Untuk kongruen pertama:

$x = 2 + 3k_1$ (iii)

Substitusikan (iii) ke dalam (ii):

$2 + 3k_1 \equiv 3 \pmod 5 \rightarrow 3k_1 \equiv 1 \pmod 5$

diperoleh

$k_1 \equiv 2 \pmod 5$ atau $k_1 = 2 + 5k_2$

Solusi

$x = 2 + 3k_1$

$\quad = 2 + 3\,(2 + 5k_2)$

$\quad = 2 + 6 + 15k_2$

$\quad = 8 + 15k_2$

atau

$x \equiv 8 \pmod{15}$

Semua nilai x yang kongruen dengan 8 (mod 15) adalah solusinya, yaitu

$x = 8$, $x = 23$, $x = 38$, …, $x = -7$, dst

Chinese Remainder Problem

- Pada abad pertama, seorang matematikawan China yang bernama Sun Tse mengajukan pertanyaan sebagai berikut:

  Tentukan sebuah bilangan bulat yang bila dibagi dengan 5 menyisakan 3, bila dibagi 7 menyisakan 5, dan bila dibagi 11 menyisakan 7.

- Misakan bilangan bulat tersebut = x. Formulasikan kedalam sistem kongruen lanjar:

$$x \equiv 3 \pmod{5}$$

$$x \equiv 5 \pmod{7}$$

$$x \equiv 7 \pmod{11}$$

Chinese Remainder Problem

Teorema 5. (*Chinese Remainder Theorem*) Misalkan m_1, m_2, …, m_n adalah bilangan bulat positif sedemikian sehingga PBB(m_i, m_j) = 1 untuk $i \neq j$. Maka sistem kongruen lanjar

$$x \equiv a_k \pmod{m_k}$$

mempunyai sebuah solusi unik dalam modulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$.

Contoh 15.

Tentukan solusi dari pertanyaan Sun Tse di atas.

Penyelesaian:

$x \equiv 3 \pmod 5$ → $x = 3 + 5k_1$ (i)

Sulihkan (i) ke dalam kongruen kedua menjadi:

$3 + 5k_1 \equiv 5 \pmod 7$ → $k_1 \equiv 6 \pmod 7$, atau $k_1 = 6 + 7k_2$ (ii)

Sulihkan (ii) ke dalam (i):

$x = 3 + 5k_1 = 3 + 5(6 + 7k_2) = 33 + 35k_2$ (iii)

Sulihkan (iii) ke dalam kongruen ketiga menjadi:

$33 + 35k_2 \equiv 7 \pmod{11}$ → $k_2 \equiv 9 \pmod{11}$ atau $k_2 = 9 + 11k_3$.

Sulihkan k_2 ini ke dalam (iii) menghasilkan:

$x = 33 + 35(9 + 11k_3) = 348 + 385k_3$

atau $x \equiv 348 \pmod{385}$. Ini adalah solusinya.

348 adalah bilangan bulat positif terkecil yang merupakan solusi sistem kekongruenan di atas. Perhatikan bahwa 348 mod 5 = 3, 348 mod 7 = 5, dan 348 mod 11 = 7. Catatlah bahwa $385 = 5 \cdot 7 \cdot 11$.

Solusi unik ini mudah dibuktikan sebagai berikut. Solusi tersebut dalam modulo:

$$m = m_1 \cdot m_2 \cdot m_3 = 5 \cdot 7 \cdot 11 = 5 \cdot 77 = 11 \cdot 35.$$

Karena $77 \,.\, 3 \equiv 1 \pmod 5$,

$55 \cdot 6 \equiv 1 \pmod 7$,

$35 \cdot 6 \equiv 1 \pmod{11}$,

maka solusi unik dari sistem kongruen tersebut adalah

$x \equiv 3 \cdot 77 \cdot 3 + 5 \cdot 55 \cdot 6 + 7 \cdot 35 \cdot 6 \pmod{385}$

$\equiv 3813 \pmod{385}$

$\equiv 348 \pmod{385}$

Bilangan Prima

- Bilangan bulat positif p ($p > 1$) disebut bilangan prima jika pembaginya hanya 1 dan p.

- Contoh: 23 adalah bilangan prima karena ia hanya habis dibagi oleh 1 dan 23.

Bilangan Prima

- Karena bilangan prima harus lebih besar dari 1, maka barisan bilangan prima dimulai dari 2, yaitu 2, 3, 5, 7, 11, 13, ….

- Seluruh bilangan prima adalah bilangan ganjil, kecuali 2 yang merupakan bilangan genap.

- Bilangan selain prima disebut bilangan **komposit** (*composite*). Misalnya 20 adalah bilangan komposit karena 20 dapat dibagi oleh 2, 4, 5, dan 10, selain 1 dan 20 sendiri.

Bilangan Prima

Teorema 6. (*The Fundamental Theorem of Arithmetic*). Setiap bilangan bulat positif yang lebih besar atau sama dengan 2 dapat dinyatakan sebagai perkalian satu atau lebih bilangan prima.

Contoh 16.

$9 = 3 \times 3$

$100 = 2 \times 2 \times 5 \times 5$

$13 = 13$ (atau 1×13)

Bilangan Prima

- Tes bilangan prima:

  (i) bagi n dengan sejumlah bilangan prima, mulai dari 2, 3, … , bilangan prima $\leq \sqrt{n}$.

  (ii) Jika n habis dibagi dengan salah satu dari bilangan prima tersebut, maka n adalah bilangan komposit,

  (ii) tetapi jika n tidak habis dibagi oleh semua bilangan prima tersebut, maka n adalah bilangan prima.

Bilangan Prima

- **Contoh 17.** Tes apakah (i) 171 dan (ii) 199 merupakan bilangan prima atau komposit.

Penyelesaian:

(i) $\sqrt{171}$ = 13.077. Bilangan prima yang $\leq \sqrt{171}$ adalah 2, 3, 5, 7, 11, 13.

Karena 171 habis dibagi 3, maka 171 adalah bilangan komposit.

(ii) $\sqrt{199}$ = 14.107. Bilangan prima yang $\leq \sqrt{199}$ adalah 2, 3, 5, 7, 11, 13.

Karena 199 tidak habis dibagi 2, 3, 5, 7, 11, dan 13, maka 199 adalah bilangan prima.

Bilangan Prima

- **Teorema 6** (**Teorema Fermat**). Jika p adalah bilangan prima dan a adalah bilangan bulat yang tidak habis dibagi dengan p, yaitu PBB(a, p) = 1, maka

$$a^{p-1} \equiv 1 \pmod{p}$$

Bilangan Prima

Contoh 18. Tes apakah 17 dan 21 bilangan prima atau bukan dengan Teorema Fermat

Ambil a = 2 karena PBB(17, 2) = 1 dan PBB(21, 2) = 1.

(i) $2^{17-1} = 65536 \equiv 1 \pmod{17}$ karena 17 habis membagi 65536 – 1 = 65535 Jadi, 17 prima.

(ii) $2^{21-1} = 1048576 \not\equiv 1 \pmod{21}$ karena 21 tidak habis membagi 1048576 – 1 = 1048575. Jadi, 21 bukan prima

Bilangan Prima

- Kelemahan Teorema Fermat: terdapat bilangan komposit n sedemikian sehingga $2^{n-1} \equiv 1 \pmod{n}$. Bilangan bulat seperti itu disebut bilangan **prima semu** (*pseudoprimes*).

- Contoh: 341 adalah komposit (karena 341 = 11 · 31) sekaligus bilangan prima semu, karena menurut teorema Fermat,

$$2^{340} \equiv 1 \pmod{341}$$

- Untunglah bilangan prima semu relatif jarang terdapat.

- Untuk bilangan bulat yang lebih kecil dari 10^{10} terdapat 455.052.512 bilangan prima, tapi hanya 14.884 buah yang merupakan bilangan prima semu terhadap basis 2.

Bilangan Prima

Hitunglah sisa pembagian 2^{2020} dibagi dengan 73

Penyelesaian: Dengan menggunakan teorema Fermat kita dapat mengetahui bahwa $2^{72} \equiv 1 \pmod{73}$.

$$
\begin{aligned}
2^{2020} &\equiv (2^{72})^{28} \cdot 2^4 \bmod 73 \\
&\equiv (1)^{28} \cdot 2^4 \bmod 73 \\
&\equiv 2^4 \bmod 73 \\
&\equiv 16 \bmod 73 = 16
\end{aligned}
$$

Jadi sisa pembagiannya adalah 16

Bilangan Prima

Tiga kemunculan terkahir komet Halley adalah pada tahun 1835, 1910, dan 1986. Kemunculan berikutnya diprediksi akan terjadi pada tahun 2061. Dengan bantuan Teorema Fermat buktikan bahwa $1835^{1910} + 1986^{2061} \equiv 0 \ (mod\ 7)$

Jawaban: Karena 7 adalah bilangan prima dan $7 \nmid 1835$ serta $7 \nmid 1986$ maka soal ini memenuhi syarat Teorema Fermat.

Selanjutnya berdasarkan teorema fermat

$1835^6 \equiv 1 \ (mod\ 7)$

$1835^{1910} \ (mod\ 7) \equiv 1835^{6*318+2} \ (mod\ 7) \equiv 1835^2 \ (mod\ 7) \equiv 1 \ (mod\ 7)$

$1986^6 \equiv 1 \ (mod\ 7)$

$1986^{2061} \ (mod\ 7) \equiv 1986^{6*343+3} \ (mod\ 7) \equiv 1986^3 \ (mod\ 7) \equiv 5^3 \ (mod\ 7) \equiv 6 \ (mod\ 7)$

Maka,

$1835^{1910} + 1986^{2061} \equiv 1 + 6 \ (mod\ 7) \equiv 0 \ (mod\ 7)$

Aplikasi Teori Bilangan

- *ISBN* (*International Book Serial Number*)
- Fungsi *hash*
- Kriptografi
- Pembangkit bilangan acak-semu
- dll

ISBN

ISBN 388053101-3

9 703880 531016

- Kode ISBN terdiri dari 10 karakter, biasanya dikelompokkan dengan spasi atau garis, misalnya 0–3015–4561–9.

- ISBN terdiri atas empat bagian kode:

  - kode yang mengidentifikasikan negara atau kelompok negara,

  - kode penerbit,

  - kode unik untuk buku tersebut,

  - karakter uji (angka atau huruf X (=10)).

ISBN

- Karakter uji dipilih sedemikian sehingga

$$\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}$$

- Karakter uji

$$\left(\sum_{i=1}^{9} i x_i\right) \bmod 11 = \text{karakter uji}$$

- Contoh: ISBN 0–3015–4561–8

  0 : kode kelompok negara berbahasa Inggris,

  3015 : kode penerbit

  4561 : kode unik buku yang diterbitkan

  8 : karakter uji.

  Karakter uji ini didapatkan sebagai berikut:

  $$1 \cdot 0 + 2 \cdot 3 + 3 \cdot 0 + 4 \cdot 1 + 5 \cdot 5 + 6 \cdot 4 + 7 \cdot 5 + 8 \cdot 6 + 9 \cdot 1 = 151$$

- Jadi, karakter ujinya adalah 151 mod 11 = 8.

Fungsi *Hash*

- Tujuan: pengalamatan di memori untuk tujuan pengaksesan data dengan cepat.

- Bentuk: $h(K) = K \bmod m$

  - m : jumlah lokasi memori yang tersedia

  - K : kunci (*integer*)

  - $h(K)$: lokasi memori untuk *record* dengan kunci unik K

Contoh: data record mahasiswa, NIM adalah kunci (*K*)

NIM	Nama	MatKul	Nilai
13598011	Amir	Matematika Diskrit	A
13598011	Amir	Arsitektur Komputer	B
13598014	Santi	Algoritma	D
13598015	Irwan	Algoritma	C
13598015	Irwan	Struktur Data	C
13598015	Irwan	Arsitektur Komputer	B
13598019	Ahmad	Algoritma	E
13598021	Cecep	Algoritma	B
13598021	Cecep	Arsitektur Komputer	B
13598025	Hamdan	Matematika Diskrit	B
13598025	Hamdan	Algoritma	A
13598025	Hamdan	Struktur Data	C
13598025	Hamdan	Arsitektur Komputer	B

Contoh: m = 11 mempunyai sel-sel memori yang diberi indeks 0 sampai 10. Akan disimpan data *record* yang masing-masing mempunyai kunci 15, 558, 32, 132, 102, dan 5.

$h(15) = 15 \bmod 11 = 4$
$h(558) = 558 \bmod 11 = 8$
$h(32) = 32 \bmod 11 = 10$
$h(132) = 132 \bmod 11 = 0$
$h(102) = 102 \bmod 11 = 3$
$h(5) = 5 \bmod 11 = 5$

132			102	15	5			558		32
0	1	2	3	4	5	6	7	8	9	10

Fungsi *Hash*

- Kolisi (*collision*) terjadi jika fungsi *hash* menghasilkan nilai *h* yang sama untuk *K* yang berbeda.

- Jika terjadi kolisi, cek elemen berikutnya yang kosong.

  Contoh: *K* = 74 → *h*(74) = 74 mod 11 = 8

132			102	15	5			558		32
0	1	2	3	4	5	6	7	8	9	10

  Oleh karena elemen pada indeks 8 sudah berisi 558, maka

  74 ditaruh pada elemen kosong berikutnya: 9

132			102	15	5			558	74	32
0	1	2	3	4	5	6	7	8	9	10

- Fungsi *hash* juga digunakan untuk me-*locate* elemen yang dicari.

Kriptografi

- Dari Bahasa Yunani yang artinya "*secret writing*"

- **Kriptografi** adalah ilmu dan seni untuk menjaga keamanan pesan dengan cara menyandikannya menjadi bentuk lain yang tidak bermakna.

- Tujuan: agar pesan yang bersifat rahasia tidak dapat dibaca oleh pihak yang tidak berhak.

Kriptografi

- **Pesan**: data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain: **plainteks** (*plaintext*)

- **Cipherteks** (*ciphertext*): pesan yang telah disandikan sehingga tidak memiliki makna lagi.

Contoh:

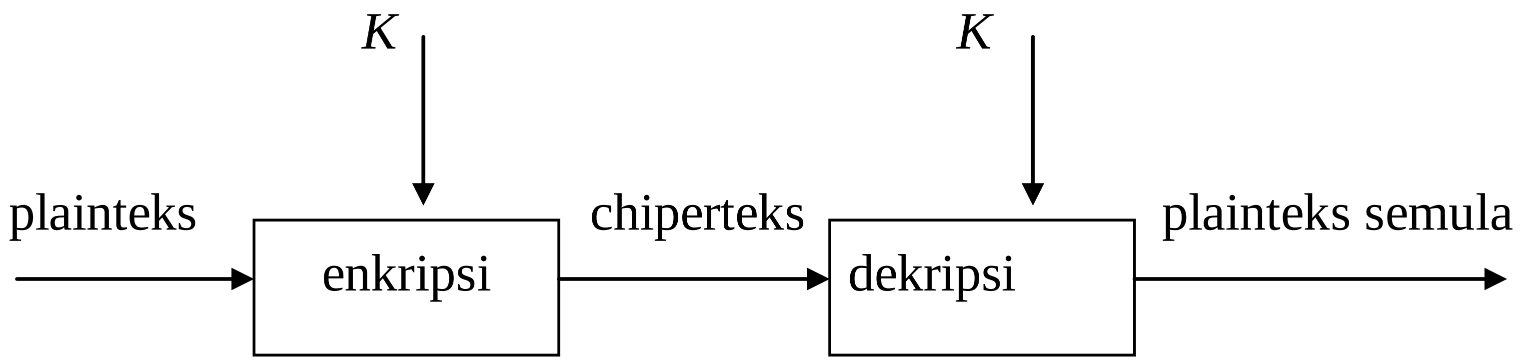
Plainteks: `culik anak itu jam 11 siang`

Cipherteks: `t^$gfUi9rewoFpfdWqL:[uTcxZy`

Kriptografi

- **Enkripsi** (*encryption*): proses menyandikan plainteks menjadi cipherteks.

- **Dekripsi** (*decryption*): Proses mengembalikan cipherteks menjadi plainteksnya.



Aplikasi Enkripsi-Deskripsi

1. Pengiriman data melalui saluran komunikasi (*data encryption on motion*).
   → pesan dikirim dalam bentuk cipherteks

2. Penyimpanan data di dalam *disk storage* (*data encryption at rest*)
   → data disimpan di dalam memori dalam bentuk cipherteks

Aplikasi Enkripsi-Deskripsi

- Data ditransmisikan dalam bentuk chiperteks. Di tempat penerima chiperteks dikembalikan lagi menjadi plainteks.

- Data di dalam media penyimpanan komputer (seperti *hard disk*) disimpan dalam bentuk chiperteks. Untuk membacanya, hanya orang yang berhak yang dapat mengembalikan chiperteks menjadi plainteks.

Contoh enkripsi pada dokumen

Plainteks (`plain.txt`):

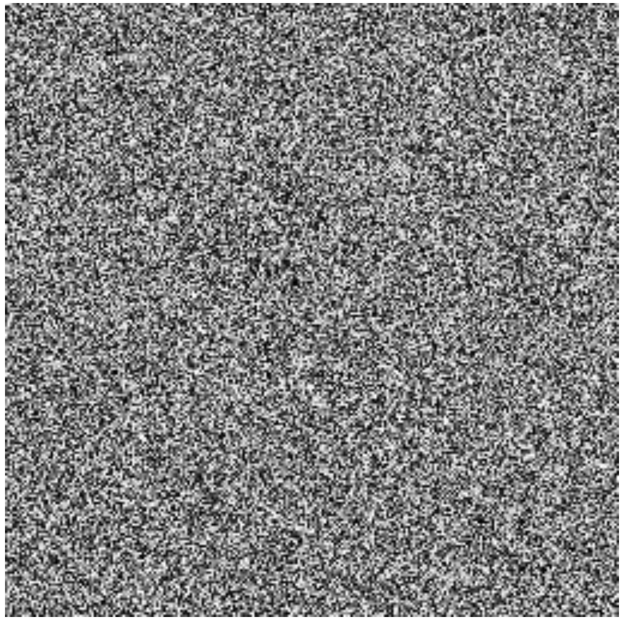
```
Ketika saya berjalan-jalan di pantai,
saya menemukan banyak sekali kepiting
yang merangkak menuju laut. Mereka
adalah anak-anak kepiting yang baru
menetas dari dalam pasir. Naluri
mereka mengatakan bahwa laut adalah
tempat kehidupan mereka.
```

Cipherteks (`cipher.txt`):

```
Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/□p}âpx;
  épêp/|t}t|äzp}/qp}êpz/étzp{x/zt□xâx
}v  êp}v/|tüp}vzpz/|t}äyä/{päâ=/\tütz
p  psp{pw/p}pz<p}pz/zt□xâx}v/êp}
v/qpüä  |t}tâpé/spüx/sp{p|/□péxü=/]
p{äüx  |ttüzp/|t}vpâpzp}/qpwåp/{päâ
/psp{pw  ât|□pâ/ztwxsä□p}/|tützp=
```

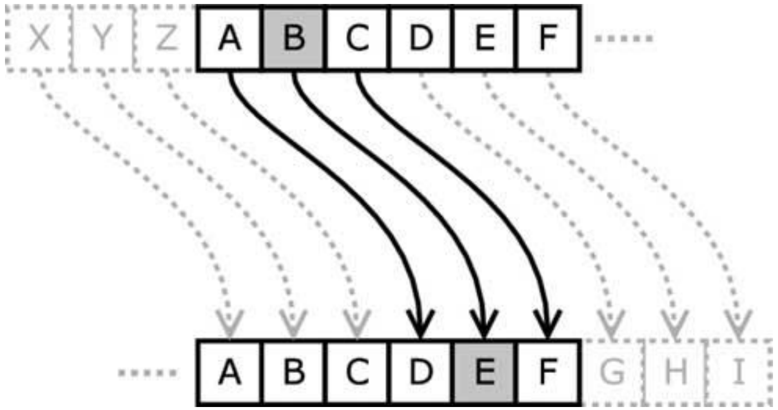
Plainteks (`lena.bmp`):

Cipherteks (`lena2.bmp`):



Caesar Cipher

- Algoritma enkripsi sederhana pada masa raja Julius Caesar
- Tiap huruf alfabet digeser 3 huruf ke kanan secara *wrapping*



Contoh: Plainteks: `AWASI ASTERIX DAN TEMANNYA OBELIX`

Cipherteks: **`DZDVL DVWHULA GDQ WHPDQQBA REHOLA`**

Caesar Cipher

- Misalkan setiap huruf dikodekan dengan angka:
  - A = 0, B = 1, C = 2, …, Z = 25

  maka secara matematis enkripsi dan dekripsi pada Caesar *cipher* dirumuskan sebagai berikut:

Enkripsi: $\boldsymbol{c_i = E(p_i) = (p_i + 3) \bmod 26}$

Dekripsi: $\boldsymbol{p_i = D(c_i) = (c_i - 3) \bmod 26}$

Caesar Cipher

Contoh:

Plainteks: `AWASI ASTERIX DAN TEMANNYA OBELIX`

Cipherteks: **`DZDVL DVWHULA GDQ WHPDQQBD REHOLA`**

p_1 = 'A' = 0 → $c_1 = E(0) = (0 + 3) \bmod 26 = 3$ = 'D'

p_2 = 'W' = 22 → $c_2 = E(22) = (22 + 3) \bmod 26 = 25$ = 'Z'

p_3 = 'A' = 0 → $c_3 = E(0) = (0 + 3) \bmod 26 = 3$ = 'D'

p_4 = 'S' = 18 → $c_4 = E(18) = (18 + 3) \bmod 26 = 21$ = 'V'

dst…

- Jika pergeseran huruf sejauh *k*, maka:

  Enkripsi: $\boldsymbol{c_i = E(p_i) = (p_i + k) \text{ mod } 26}$

  Dekripsi: $\boldsymbol{p_i = D(c_i) = (c_i - k) \text{ mod } 26}$

  k = kunci rahasia

- Pada *Caesar Cipher*, *k* = 3
- Untuk alfabet ASCII 256 karakter,

  Enkripsi: $\boldsymbol{c_i = E(p_i) = (p_i + k) \text{ mod } 256}$

  Dekripsi: $\boldsymbol{p_i = D(c_i) = (c_i - k) \text{ mod } 256}$

``program enkripsi;
{ Mengenkripsi berkas 'plain.txt'
  menjadi 'cipher.txt' dengan
  metode caesar cipher }
uses
  crt;
var
   F1, F2 : text;
   p : char;
   c : integer;
   k : integer;
 	
begin
   assign(F1, 'plain.txt');
   reset(F1);
 	
   assign(F2, 'cipher.txt');
   rewrite(F2);
 	
   write('k = ?'); readln(k);
   while not EOF(F1) do
    begin
      while not EOLN(F1) do
       begin
         read(F1, p);
         c := (ord(p) + k) mod 256;
         write(F2, chr(c));
       end;
      readln(F1);
      writeln(F2);
   end;
   close(F1);
   close(F2);
end.```
	``program dekripsi;
	{ Mendekripsi berkas 'cipher.txt'
	  menjadi 'plain2.txt' dengan
	  metode caesar cipher }
	uses
	  crt;
	var
	   F1, F2 : text;
	   p : char;
	   c : integer;
	   k : integer;
	
	begin
	   assign(F1, 'cipher.txt');
	   reset(F1);
	
	   assign(F2, 'plain2.txt');
	   rewrite(F2);
	
	   write('k = ?'); readln(k);
	   while not EOF(F1) do
	    begin
	      while not EOLN(F1) do
	       begin
	         read(F1, p);
	         c := (ord(p) - k) mod 256;
	         write(F2, chr(c));
	       end;
	      readln(F1);
	      writeln(F2);
	   end;
	   close(F1);
	   close(F2)
	end.```

Algoritma RSA

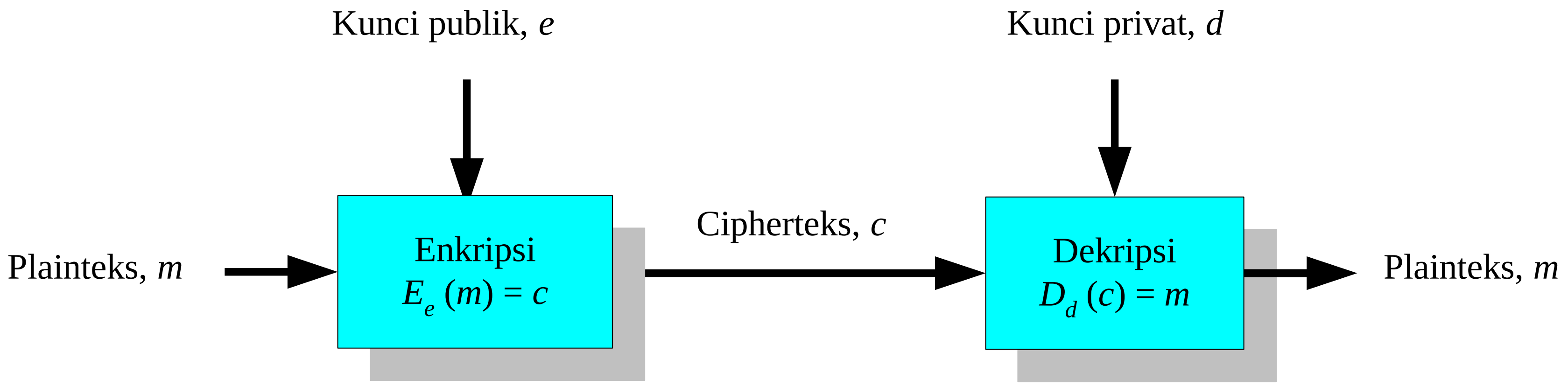
- Dibuat oleh tiga peneliti dari *MIT* (*Massachussets Institute of Technology*), yaitu Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976.

- Termasuk algoritma **kriptografi asimetri**.
- Asimetri: kunci untuk enkripsi berbeda dengan kunci untuk dekripsi

Algoritma RSA

- Setiap pengguna memiliki sepasang kunci:
  1. Kunci publik, *e*: untuk enkripsi pesan
  2. Kunci privat, *p*: untuk dekripsi pesan

- Kunci publik tidak rahasia, kunci privat rahasia



Algoritma RSA

Algoritma pembangkitan pasangan kunci

1. Pilih dua bilangan prima, p dan q (rahasia)
2. Hitung $n = pq$. Besaran n tidak perlu dirahasiakan.
3. Hitung $m = (p - 1)(q - 1)$.
4. Pilih sebuah bilangan bulat untuk kunci publik, e, relatif prima terhadap m.
5. Hitung kunci dekripsi, d, melalui kekongruenan $ed \equiv 1 \ (\mathbf{mod}\ m)$.

Algoritma RSA

- **Contoh.** Misalkan p = 47 dan q = 71 (keduanya prima), maka dapat dihitung

$$n = p \times q = 3337$$

$$m = (p - 1)\times(q - 1) = 3220.$$

Pilih kunci publik e = 79 (yang relatif prima dengan 3220.

Nilai e dan n dapat dipublikasikan ke umum.

- **Catatan**: Dalam praktek, nilai a, b, dan e adalah bialngan yang sangat besar (minimal 200 digit)

Algoritma RSA

- Selanjutnya dihitung kunci dekripsi *d* dengan kekongruenan:

$$e \times d \equiv 1 \pmod{m}$$

$$d = \frac{1 + (k \times 3220)}{79}$$

Diperoleh nilai *d* = 1019. Ini adalah kunci dekripsi.

Algoritma RSA

Algoritma enkripsi-dekripsi:

Enkripsi: $c_i = p_i^e \textbf{ mod } n$

Dekripsi: $p_i = c_i^d \textbf{ mod } n$,

Algoritma RSA

- Misalkan plainteks: ‘HARI INI’

  atau dalam desimal ASCII: 7265827332737873

  Pecah pesan menjadi blok yang lebih kecil (misal 3 digit):

  $p_1 = 726$ $p_4 = 273$
  $p_2 = 582$ $p_5 = 787$
  $p_3 = 733$ $p_6 = 003$

Algoritma RSA

- *Enkripsi setiap blok:*

  $c_1 = 726^{79} \bmod 3337 = 215$

  $c_2 = 582^{79} \bmod 3337 = 776$

  dst untuk sisa blok lainnya

  Keluaran: chiperteks C = 215 776 1743 933 1731 158.

- *Dekripsi (menggunakan kunci privat d = 1019)*

  $p_1 = 215^{1019} \bmod 3337 = 726$

  $p_2 = 776^{1019} \bmod 3337 = 582$

  dst untuk sisi blok lainnya

  Keluaran: plainteks = 7265827332737873

  atau dalam kode ASCII karakternya adalah HARI INI.

Latihan Soal - 1

Sebuah buku terbitan September 2008 memiliki ISBN 9**X**7-2309-97. Tentukan nilai X dan karakter uji dari nomor ISBN tersebut jika diketahui $3X \equiv 2 (mod\ 5)$

Jawaban - 1

$$3X \equiv 2(mod\ 5) \longrightarrow X = \frac{2+5k}{3}$$

Untuk nilai k =

k = 1 → X = 2/3
k = 2 → X = 4
k = 3 → X = 17/3
k = 4 → X = 22/3
k = 5 → X = 9
k = 6 → X = 32/3
k = 7 → X = 37/3
k = 8 → X = 14

...dst

Dapat dilihat di atas, untuk k = 2, 5, 8, ... nilai X bulat, namun untuk kode ISBN di atas, nilai X haruslah dalam rentang bilangan bulat 0-9, jadi nilai X yang memenuhi adalah **4** dan **9**.

Jawaban - 1

Untuk mencari karakter uji, diketahui

$\sum_{i=i}^{9} ix_i$ mod 11 = karakter uji

Maka nilai karakter uji untuk :

kode ISBN 9**4**7-2309-97 dapat dicari sebagai berikut :

$$\sum_{i=i}^{9} ix_i = 1(9) + 2(4) + 3(7) + 4(2) + 5(3) + 6(0) + 7(9) + 8(9) + 9(7) = 259$$

Jadi karakter uji untuk ISBN di atas = 259 mod 11 = **6**

kode ISBN 9**9**7-2309-97 dapat dicari sebagai berikut :

$$\sum_{i=i}^{9} ix_i = 1(9) + 2(9) + 3(7) + 4(2) + 5(3) + 6(0) + 7(9) + 8(9) + 9(7) = 269$$

Jadi karakter uji untuk ISBN di atas = 269 mod 11 = **5**

Latihan Soal - 2

Sebuah area parkir mempunyai sejumlah *slot* atau *space* yang dinomori 0 sampai 25. Mobil yang hendak parkir di area tersebut ditentukan dengan sebuah fungsi *hash*. Fungsi *hash* tersebut menentukan nomor *slot* yang akan ditempati mobil yang hendak parkir berdasarkan 3 angka terakhir pada plat nomor polisinya.

(a) Tentukan fungsi *hash* yang dimaksudkan.

(b) Tentukan nomor *slot* yang ditempati mobil yang datang berturut-turut dengan plat nomor polisinya adalah 423251, 76540, 17121, 2310, 4124, 1102, 1724

Jawaban - 2

(a) $h = x \bmod 26$

(b) 423251 → 3 angka terakhir = 251 → 251 mod 26 = 17 (slot 17)

76540 → 3 angka terakhir = 540 → 540 mod 26 = 20 (slot 20)

17121 → 3 angka terakhir = 121 → 121 mod 26 = 17

(tetapi slot nomor 17 sudah terisi, jadi isi slot kosong berikutnya, yaitu 18)

2310 → 3 angka terakhir = 310 → 310 mod 26 = 24 (slot 24)

4124 → 3 angka terakhir = 124 → 124 mod 26 = 20

(slot 21 karena slot 20 sudah terisi)

1102 → 3 angka terakhir = 102 → 102 mod 26 = 24

(slot 25 karena slot 24 sudah terisi)

1724 → 3 angka terakhir = 724 → 724 mod 26 = 22 (slot 22)

Jadi, mobil-mobil yang datang mengisi slot 17, 20, 18, 24, 21, 25, dan 22

Latihan Soal - 3

- Tentukan x dan y bilangan bulat yang memenuhi persamaan $312x + 70y = 2$, lalu hitunglah nilai dari : y mod x .

Jawaban - 3

Dengan menggunakan algoritma Euclid, ditemukan bahwa :

312 = 4.70 + 32 (i)

70 = 2.32 + 6 (ii)

32 = 5.6 + 2 (iii)

6 = 3.2 + 0 (iv)

Persamaan (iii) dapat dituliskan menjadi : 2 = 32 – 5.6 (v)

Persamaan (ii) dapat dituliskan menjadi : 6 = 70 – 2.32 (vi)

Sulihkan persamaan (vi) ke persamaan (v) :

2 = 32 – 5.(70 – 2.32)

2 = 32 – 5.70 + 10.32

2 = 11.32 – 5.70 (vii)

Persamaan (i) dapat dituliskan menjadi : 32 = 312 – 4.70 (viii)

REFERENSI

1. Dr. Ir. Rinaldi Munir, M.T, *Matematika Diskrit (Edisi Kelima*), Bandung: Informatika , 2013.