II4021 Kriptografi

02 - Landasan Matematika untuk Kriptografi

Oleh: Rinaldi M

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2026

Materi Matematika untuk Kriptorafi:

1. Teori Bilangan
   - Integer dan aritmetika modulo
   - Algoritma euclidean
   - Kekongruenan
   - Relatif prima
   - Balikan (invers) modulo
   - Bilangan prima

2. Probabilitas dan Statistik

3. Kompleksitas algoritma

4. Teori Informasi

5. Aljabar abstrak

No. 1 s/d 3 sudah dipelajari di dalam kuliah Matematika Diskrit dan Probabilitas dan Statistik

No 5 akan dibahas pada materi *ECC* (*Elliptic Curve Cryptography*)

Contoh:

(i) 23 **mod** 5 = 3 karena 23 dibagi 5 = 4 + sisa 3

(ii) –41 **mod** 9 = 4 karena |-41| mod 9 = 5, dan 9 – 5 = 4

(iii) $17 \equiv 2$ (**mod** 3) karena 3 | (17 – 2)

(iv) $-7 \equiv 15$ (**mod** 11) karena 11 | (-7 – 15)

(v) 23 dan 40 relatif prima sebab PBB(23, 4) = 1

(vi) 4^{-1} (**mod** 9) $\equiv 7$ (mod 9) karena $4 \cdot 7 \equiv 1$ (mod 9)

(vii) 23^{-1} (**mod** 10) = -3 (mod 10) karena $23 \cdot (-3) \equiv 1$ (mod 10)

Latihan: (a) Hitung -24 **mod** 11 = ?

(b) 12^{-1} (**mod** 5) $\equiv$?

Teori Informasi (*Information Theory*)

- *Information theory*: cabang ilmu yang mempelajari **kuantisasi, penyimpanan, transmisi, dan pengolahan informasi**

- Contoh kuantisasi:
  - 1 bit untuk mengkodekan jenis kelamin (M/F)
  - 3 bit untuk mengkodekan nama hari (ada 7 hari)
  - 4 bit untuk mengkodekan 0 s/d 9

- Contoh penyimpanan: pemampatan data untuk mengurangi ukuran ruang *storage*

- Salah satu metrik penting di dalam teori informasi adalah **entropi**.
- **Entropi** mengukur *ketidakpastian* atau jumlah rata-rata informasi di dalam pesan.
- Semakin acak suatu data, semakin tinggi entropinya. Cipherteks adalah pesan dengan entropi yang tinggi.
- Entropi biasanya dinyatakan dalam satuan bit.
- Secara umum, entropi pesan X dihitung dengan rumus:

$$H(X) = -\sum_{i=1}^{n} p(x_i)\ \log_2\ p(x_i)$$

X = variabel acak yang menyatakan pesan

x_i = simbol ke-i di dalam pesan

n = banyak simbol di dalam pesan

$p(x_i)$ = peluang kemunculan x_i

- Contoh: misalkan pesan X = ‘AABBCBDB’

  $n = 4$ (yaitu huruf A, B, C, D)

  $p(A) = 2/8$, $p(B) = 4/8$

  $p(C) = 1/8$, $p(D) = 1/8$

$$H(x) = -\{2/8\ {}^2\log(2/8) + 4/8\ {}^2\log(4/8) + 1/8\ {}^2\log(1/8) + 1/8\ {}^2\log(1/8)\ \}$$

$$= -\{1/4\ {}^2\log(1/4) + 1/2\ {}^2\log(1/2) + 1/8\ {}^2\log(1/8) + 1/8\ {}^2\log(1/8)\ \}$$

$$= -\{(1/4)\ (-\ {}^2\log(4) + (1/2)\ (-\ {}^2\log(2) + (1/8)\ (-\ {}^2\log(8) + (/8)\ (-\ {}^2\log(8)\ \}$$

$$= -\{(1/4)\ (-\ 2) + (1/2)\ (-1) + (1/8)\ (-3) + (1/8)(-3)\ \}$$

$$= -\ \{-1/2 – 1/2 – 3/8 – 3/8)$$

$$= -\ (-1.75)$$

$$= 1.75$$

Entropi = 1,75 bit per simbol

- Nilai entropi berkisar dalam rentang:

$$0 \leq H(X) \leq \log_2(n)$$

- Entropi minimum = 0 bit

  $\rightarrow$ Tidak ada ketidakpastian

  $\rightarrow$ Terjadi jika hanya ada satu simbol dengan peluang 1 (pasti).

  Contoh: n = 1, misalkan A dan p(A) =1 $\rightarrow$ H(X) = $-1 \cdot \log_2 1 = 0$

- Entropi maksimum = $\log_2(n)$ bit

  $\rightarrow$ Terjadi jika semua simbol muncul dengan peluang sama, yaitu 1/n.

  $\rightarrow$ Ketidakpastian paling tinggi, setiap simbol membawa informasi maksimal.

  Contoh: Empat simbol dengan peluang sama (0.25) $\rightarrow$ $H(X) = -\sum_{i=1}^{4} 0.25 \log_2 0.25 = 2 \text{ bit}$

- Entropi sistem kriptografi adalah ukuran kunci, *K*.
- Misal, sistem kriptografi AES dengan kunci 128-bit mempunyai entropi 128 bit.
- Makin besar entropi, makin sulit memecahkan cipherteks.