

IF4020 Kriptografi

Landasan Matematika untuk Kriptografi

Oleh: Dr. Rinaldi Munir

**Prodi Informatika
Sekolah Teknik Elektro dan Informatika
2021**

Pendahuluan

- Perlu landasan matematika untuk mempelajari kriptografi.
- Materi matematika yang utama untuk kriptografi adalah **matematika diskrit** dan **probabilitas dan statistika**.

Materi Matematika untuk Kriptografi:

1. Teori Bilangan
 - Integer dan sifat-sifat pembagian
 - 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) $23 \bmod 5 = 3$

(ii) $-41 \bmod 9 = 4$

(iii) $17 \equiv 2 \pmod{3}$

(iv) $-7 \equiv 15 \pmod{11}$

(v) 23 dan 40 relatif prima sebab $\text{PBB}(23, 4) = 1$

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

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

Latihan: (a) Hitung $-24 \bmod 11 = ?$

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

Teori Informasi

- Mendefinisikan jumlah informasi di dalam pesan sebagai jumlah minimum bit yang dibutuhkan untuk mengkodekan pesan.
- Contoh:
 - 1 bit untuk mengkodekan jenis kelamin
 - 3 bit untuk mengkodekan nama hari
 - 4 bit untuk mengkodekan 0 s/d 9

- *Entropy*: ukuran yang menyatakan jumlah informasi di dalam pesan.
- Biasanya dinyatakan dalam satuan bit.

- Entropi berguna untuk memperkirakan jumlah bit rata-rata untuk mengkodekan elemen dari pesan.

- Contoh: entropi untuk pesan yang menyatakan jenis kelamin = 1 bit, entropi untuk pesan yang menyatakan nama hari = 3 bit

- Secara umum, entropi pesan dihitung dengan rumus:

$$H(X) = -\sum_{i=1}^n a_i \log(p(S_i))$$

X = pesan

S_i = simbol ke- i di dalam pesan

$p(S_i)$ = peluang kemunculan S_i

a_i = jumlah kemunculan S_i

- Contoh: misalkan pesan $X = \text{'AABBCBDB'}$

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

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

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

$$\begin{aligned} H(x) &= -2^2 \log(2/8) - 4^2 \log(4/8) - 1^2 \log(1/8) - 1^2 \log(1/8) \\ &= 4 + 4 + 3 + 3 = 14 \text{ bit} \end{aligned}$$

Entropi rata-rata = $14/4 = 1,75$ bit per simbol

- Entropi sistem kriptografi adalah ukuran kunci, K .
- Misal, sistem kriptografi dengan kunci 64-bit mempunyai entropi 64 bit.
- Makin besar entropi, makin sulit memecahkan cipherteks.

- Laju bahasa (*rate of a language*):

$$r = H(X)/N$$

N = panjang pesan

- Pada contoh sebelumnya, $X = \text{'AABBCBDB'}$, $H(X) = 14$, $N = 8$, maka

$$r = 14/8 = 1.75$$

- Laju normal Bahasa Inggris:

1.0 bit/huruf s/d 1.5 bit/huruf untuk N besar.

- Laju mutlak (*absolute rate*):

$$R = \log_2 L$$

L = jumlah karakter di dalam bahasa

- Dalam Bahasa Inggris (26 huruf):

$$R = \log_2 26 = 4.7 \text{ bit/huruf}$$

- Redundansi bahasa (D):

$$D = R - r$$

- Pada Bahasa Inggris ($r = 1.3$):

$$D = 4.7 - 1.3 = 3.4 \text{ bit/huruf}$$

artinya setiap huruf dalam Bahasa Inggris membawa 3.4 bit informasi redundan (mubazir)

- Pada pesan ASCII (256 karakter):

$$R = {}^2\log 256 = 8$$

$$r = 1.3 \text{ (sama seperti B. Inggris)}$$

$$D = 8 - 1.3 = 6.7 \text{ bit/karakter}$$

- Kriptanalisis menggunakan redundansi alami dari bahasa untuk mengurangi kemungkinan jumlah plainteks.
- Contoh: kata “dan” dalam B. Indonesia redundan. Misalnya jika di dalam cipherteks banyak muncul kriptogram “ftY” (3 huruf) maka kemungkinan besar itu adalah “dan”.
- Makin besar redundansi bahasa, makin mudah melakukan kriptanalisis.

- Dalam dunia-nyata, implementasi kriptografi dilengkapi dengan program kompresi sebelum mengenkripsi pesan.
- Kompresi mengurangi redundansi pesan.