Penerapan Kombinatorika pada Kriptografi dan Jenis-Jenis Teknik Kriptografi

Muhammad Naufal - 13514073
Program Sarjana Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13514073@std.stei.itb.ac.id

***Abstrak* — Komunikasi merupakan sesuatu yang sangat penting saat ini. Untuk itu, diperlukan suatu cara untuk mengamankan komunikasi tesebut agar tidak disalahgunakan oleh pihak yang tidak berkepentingan. Kritografi adalah jawaban dari masalah tersebut. Kritografi menggunakan berbagai teknik aritmatika untuk mengubah teks agar terhindar dari penyalahgunaan oleh yang tidak berkepentigan.**

***Kata Kunci* — Kriptografi, Komunikasi.**

I. PENDAHULUAN

A. Kriptografi

Kriptografi adalah ilmu yang mempelajari cara untuk mengamankan atau merahasiakan berita yang akan disampaikan. Kriptografi berasal dari bahasa Yunani *kryptos* yang berarti rahasia dan *graphein* yang berarti tulisan.

Kriptografi sudah digunakan sejak zaman dahulu. Pada saat itu, kriptografi digunakan untuk mengamankan pesan dari musuh. Teknik penyandian yang paling terkenal saat itu adalah sandi transposisi dan sandi substitusi. Sedangkan penggunaan kriptografi pada saat ini sangat banyak, contohnya untuk mengamankan telepon genggam, akun *email*, dan lain-lain.

II. DASAR TEORI

A. Aritmatika Modulo

Modulo merupakan operasi yang digunakan untuk mencari sisa pembagian. Misalkan 27 dibagi 5 menghasilkan 5 dengan sisa 2, dapat ditulis dalam operasi modulo sebagai 27 mod 5 ≡ 2. Definisi dari operasi mod adalah:

Misalkan a adalah bilangan bulat dan m adalah bilagan bulat > 0. Maka a mod m = r sedemkian sehingga a = mq + r, dengan 0 <= r < m.

B. Kombinatorika

Kombinatorika adalah cabang ilmu matematika yang mempelajari tentang struktur diskrit. Di dalam kombinatorika, kita harus menghitung semua kemungkinan pengaturan objek. Dua kaidah dasar yang digunakan dalam kombinatorika adalah kaidah perkalian dan kaidah penjumlahan.

1. Kaidah perkalian

Bila percobaan 1 dapat dilakukan dengan p cara, dan percobaan 2 dapat dilakukan dengan q cara, maka apabila ingin melakukan percobaan 1 dan 2, dapat dilakukan dengan $p \times q$ cara.

2. Kaidah penjumlahan

Bila percobaan 1 dapat dilakukan dengan p cara, dan percobaan 2 dapat dilakukan dengan q cara, maka apabila ingin melakukan percobaan 1 atau 2, dapat dilakukan dengan $p + q$ cara.

3. Permutasi

Permutasi merupakan jumlah cara yang dapat digunakan untuk menyusun sekumpulan objek dengan memperhatikan letak dari objek tersebut. Permutasi r dari n dapat dihitung dengan cara P(n, r) = n! / (n - r)!

4. Kombinasi

Kombinasi merupakan jumlah cara yang dapat digunakan untuk menyusun sekumpulan objek tanpa memperhatikan letak dari objek tersebut. Kombinasi n dari r dapat dihitung dengan cara C(n, r) = n! / ((n - r)! x r!).

III. ISTILAH-ISTILAH KRIPTOGRAFI

Untuk mengetahui lebih dalam mengenai kriptografi, kita harus mengetahui berbagai istilah yang digunakan dalam dunia tersebut, istilah-istilah dasar yang harus dipahamai antara lain adalah:

a. Plaintext

Plaintext adalah text atau pesan yang akan dienkripsi.

b. Ciphertext

Ciphertext merupakan text yang sudah diubah.

c. Key

Key merupakan kalimat atau teks yang digunakan untuk kriptografi.

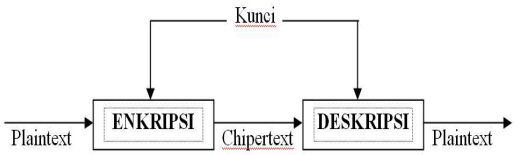
d. Enkripsi

Enkripsi merupakan *key (*kunci) yang digunakan untuk mengubah plaintext menjadi ciphertext.

e. Deskripsi

Deskripsi merupakan key (kunci) yang digunakan untuk mengembalikan ciphertext menjadi plaintext kembali.

Pada diagram dibawah ini diperlihatkan hubungan antar semua istilah di atas:



Gambar 2. 1 - Enkripsi dan Deskripsi

IV. KLASIFIKASI TEKNIK KRIPTOGRAFI

A. Berdasarkan Era Pengembangan

Berdasarkan waktu penggunaannya, teknik kriptografi dapat dikategorikan dalam dua jenis, yaitu:

1. Kriptografi Klasik

Kriptografi klasik adalah teknik kriptografi yang digunakan sebelum era digital.

2. Kriptografi Modern

Kriptografi modern merupakan teknik kriptografi yang digunakan pada era digital. Algoritma ini memiliki kompleksitas yang luar biasa

B. Berdasarkan Kesimetrisan

Berdasarkan kuncinya, teknik kriptografi dapat digolongkan dalam dua jenis, yaitu:

1. Algoritma Simetris

Algoritma Simetris adalah algoritma yang kunci yang digunakan untuk dan enkripsi dan deskripsi sama. Key dalam algoritma ini bersifat rahasia. Contoh algoritma simetris adalah:

- DES
- IDEA
- FAL

2. Algoritma Asimetris

Algoritma Asimetris adalah algoritma yang kunci yang digunakan untuk enkripsi dan deskripsi berbeda. Enkripsi yang digunakan pada algoritma ini bersifat publik, sedangkan Deskripsi yang digunakan pada algoritma ini bersifat rahasia. Contoh algoritma asimetrsi adalah:

- RSA
- DSA
- Diffie-Hellman (DH)

V. TEKNIK KRIPTOGRAFI

A. Teknik Substitusi

Pada Teknik Substitusi, setiap satu unit pada plaintext disubstitusi dengan satu unit ciphertext. Satu unit dapat berarti satu huruf, pasangan huruf, atau lebih dari dua huruf.

B. Caesar Cipher

Algoritma ini merupakan teknik yang digunakan pada zaman Kaisar Romawi, Julius Caesar, untuk menyandikan pesan yang ia kirimkan kepada bawahannya. Setiap huruf pada pesan digeser tergantung pada angka yang digunakan.

Contoh:
Misalkan semua huruf akan dishift dengan angka 5, maka teks “Saya senang belajar matematika diskrit” menjadi:

“Xfdf xjsfsl gjqfofw rfyjrfynpf inxpwny”

Interpretasi matematika dari algoritma ini adalah: Misalkan dengan mengkodekan setiap huruf dengan bilagan bulat: ‘A’ = 0, ‘B’ = 1, … ‘Z’ = 25, maka dengan pergeseran 5 huruf ekivalen dengan melakukan operasi modulo terhadap plaintext p dengan ciphertext c

$c = e(p) = (p + 5) \bmod 26$

C. Reverse Cipher

Algoritma ini sangat sederhana. Setiap kata diubah sehingga huruf pertama menjadi huruf terakhir, huruf kedua menjadi kedua terakhir, dan seterusnya.

Contoh:
Misalkan plaintext P = “Saya senang belajar

matematika diskrit", maka ciphertext C = "Ayas gnanes rajaleb akitametam tirksid".

D. Vigenere Cipher

Vigenere Cipher merupakan algoritma yang ditemukan oleh seorang diplomat sekaligus kriptolog (orang yang mendalami ilmu kriptografi) Perancis bernama Blaise de Vigenere pada abad ke-19. Cipher ini menggunakan Vigenere table untuk melakukan substitusi. Vigenere table dapat dilihat pada gambar di bawah:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 3. Vigenere Table

Setelah itu tentukan key yang akan digunakan. Jika key lebih pendek dari plaintext, maka key akan diulang-ulang.

Contoh:
Misalkan Plaintext P = "MAKAN NASI" dan Key yang digunakan adalah = "ENAK".

Plaintext : MAKAN NASI
Key : ENAKE NAKE

Maka Ciphertext merupakan huruf yang didapatkan di persilangan plaintext dan key pada Vigenere Table. Maka didapatkan

Ciphertext: QNKKR AACM.

E. DES

DES merupakan algoritma *cipher block* yang pernah populer pada saat dikembangkan pada tahun 1972. Algoritma ini beroperasi pada 64-bit. Akan tetapi, dari 64-bit tersebut hanya 56-bit saja yang digunakan untuk proses enkripsi. Maka akan terdapat 2^{56} atau 72.057.594.037.927.936 kemungkinan kunci.

F. RSA

Algoritma ini dikembangkan oleh tiga orang peneliti dari MIT (Massachussets Institute of Technology), yaitu Ron Rivest, Adi Shamir, dan Led Adleman, pada tahun 1976. Nama algoritma ini diambil dari inisial ketiga penemu tersebut (RSA: Rivest-Shamir-Adleman). RSA menggunakan konsep bilangan prima dan modulo aritmetika.

Algoritma RSA

Pemilihan kunci

1. Pilih dua bilangan prima berbeda a dan b.
2. Hitung n = a x b
3. Hitung m = (a - 1)(b - 1)
4. Pilih bilangan bulat antara satu dan m (1 < e < m) yang harus relatif prima terhadap m.
5. Hitung d sehingga d x e ≡ 1 (mod m)

Enkripsi

1. Buatlah plaintext menjadi kelompok-kelompok: p_1, p_2, .. (i harus dalam himpunan 0, 1, 2, … n - 1)
2. Hitung ci untuk pi dengan rumus:

$$\mathbf{ci = p_i^e \bmod n}$$

Deskripsi

1. Proses ini dilakukan dengan menggunakan rumus:

$$\mathbf{pi = c_i^d \bmod n}$$

VI. KESIMPULAN

Kriptografi sudah dikenal dan digunakan sejak zaman dahulu. Ini menandakan bahwa kriptografi merupakan ilmu yang sangat diperlukan. Dengan menggunakan ilmu kombinatorika, kita dapat menerapkan teknik kriptografi tersebut.

VII. UCAPAN TERIMA KASIH

Pertama, saya ingin bersyukur kepada Tuhan Yang Maha Esa karena dengan bantuan-Nya saya dapat menyelesaikan makalah ini dengan tepat waktu. Saya juga ingin mengucapkan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir dan Ibu Dra. Harlili, M. Sc. yang telah membimbing saya dan teman-teman pada mata kuliah IF2120 Matematika Diskrit ini. Dan juga saya berterima

kasih kepada orang tua saya, yang telah membiayai saya, sehingga saya dapat belajar dengan sungguh-sungguh.

DAFTAR PUSTAKA

http://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jenis-kriptografi.html, dikases pada 10 Desember 2015.

http://kriptografi-bsi.blogspot.co.id/2013/05/istilah-istilah-dalam-kriptografi.html, diakses pada 11 Desember 2015.

http://kriptografi-bsi.blogspot.co.id/2013/06/jenis-jenis-kriptografi.html, diakses pada 11 Desember 2015.

https://darhafm.wordpress.com/2012/05/07/43/ diakses pada 11 Desember 2015.

Munir, Rinaldi. 2009. Matematika Diskrit. Bandung : Informatika.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 10 Desember 2015

Muhammad Naufal
NIM: 13514073