Aplikasi Teori Bilangan pada Kriptografi

Dwi Kalam Amal Tauhid 13519210[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13519210@std.stei.itb.ac.id

***Abstrak*—Pemaparan terkait pengaplikasian konsep teori bilangan pada dua model kriptografi, yaitu Kriptografi Caesar Chiper dan Kriptografi Kunci-Publik RSA, serta dibahas dan dianalisis kedua model kriptografi tersebut.**

***Keywords*—Caesar Chiper, kriptografi, Kunci-Publik RSA, Teori Bilangan.**

I. PENDAHULUAN

Sejak zaman dahulu, konsep kriptografi telah diaplikasikan untuk mengenkripsi pesan yang hendak dikirim atau diterima. Hal tersebut sangat bermanfaat dalam menjaga privasi seseorang, baik terkait identitasnya, dokumen-dokumen yang sifatnya privasi, dan lain sebagainya.

Dewasa ini, orang-orang pada umumnya saling terhubung dan memiliki kemudahan dalam mengakses apa pun sehingga kehadiran kriptografi sangatlah diperlukan.

Oleh karenanya, penulis sangat tertarik untuk membahas konsep-konsep dasar pemodelan kriptografi. Melalui makalah ini, penulis memaparkan konsep teori bilangan dan pengimplementasiannya terhadap dua model kriptografi, yaitu Kriptografi Caesar Chiper dan Kriptografi Kunci-Publik RSA.

II. LANDASAN TEORI

A. Teori Bilangan

Teori bilangan adalah cabang matematika murni yang ditujukan untuk mempelajari bilangan bulat atau fungsi bernilai bilangan bulat. Contoh bilangan bulat adalah 8, 21, 24, -5, dan 0.

B. Sifat Pembagian pada Bilangan Bulat

Misalkan a dan b adalah bilangan bulat dengan $a \neq 0$.

a dikatakan habis membagi b jika terdapat bilangan bulat c sedemikian sehingga $b = ac$.

Notasi: $a \mid b$ jika $b = ac$, $c \in \boldsymbol{Z}$ dan $a \neq 0$.

C. Pembagi Bersama Terbesar (PBB)

Misalkan a dan b adalah bilangan bulat tidak nol.

Pembagi bersama terbesar dari a dan b adalah bilangan bulat terbesar d sedemikian sehingga $d \mid a$ dan $d \mid b$.

Notasi: PBB(a, b) = d.

Menentukan berapa pembagi bersama terbesar antara bilangan bulat tidak nol a dan b dapat ditentukan dengan memanfaatkan algoritma Euclidean.

- Algotima Euclidean

Diberikan dua buah bilangan bulat tidak negatif m dan n (m ≥ n). Berikut adalah algoritma Euclidean untuk mencari pembagi bersama terbesar dari m dan n.

1. Jika $n = 0$ maka m adalah PBB(m,n); stop.
   Tetapi, jika n ≠ 0 maka 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 ulangi kembali ke langkah 1.

D. Relatif Prima

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

E. Kongruen

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

$a \equiv b \pmod m$ dibaca "a kongruen dengan b dalam modulus m."

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

Beberapa sifat-sifat dari kekongruenan adalah sebagai berikut.

(1) $a \equiv b \pmod m$ iff $b \equiv a \pmod m$
(2) $a \equiv (b + c) \pmod m$ iff $(a - c) \equiv b \pmod m$
(3) $a \equiv b \pmod m$ dan $c \equiv d \pmod m$ maka $(a + c) \equiv (b + d) \pmod m$
(4) $a \equiv b \pmod m$ dan $c \in \boldsymbol{Z}$ maka $ac \equiv bc \pmod m$
(5) $a \pm mk \equiv a \pmod m, k \in \boldsymbol{Z}$

III. PEMBAHASAN

A. Kriptografi Caesar Chiper

Salah satu konsep kriptografi tertua adalah kriptografi Caesar Chiper. Caesar Chiper menuliskan suatu teks yang dienkripsikan dengan cara "menggeser" tiap-tiap huruf alfabet pada pesannya sejauh 3 huruf.

Misalkan huruf-huruf alfabet turut direpresentasikan dengan bilangan bulat sebagai indeks. 0 sebagai representasi huruf A, 1 sebagai representasi huruf B, hingga 25 sebagai representasi huruf Z.

Huruf	A	B	C	D	E	F	G	H	I	…
Indeks	0	1	2	3	4	5	6	7	8	…

Tabel 1. Representasi tiap huruf dengan angka.

Setelah dilakukan pergeseran sejauh 3 huruf, urutan alfabet semula terhadap alfabet hasil pergeseran menjadi:

Awal	A	B	C	D	E	F	G	H	I	…
Akhir	D	E	F	G	H	I	J	K	L	…

Tabel 2. Representasi alfabet awal terhadap alfabet hasil pergeseran.

Dengan menggunakan konsep kekongruenan pada teori bilangan, secara umum dapat dituliskan rumus dalam pengenkripsian kriptografi tersebut:

$C \equiv (P + 3)\ (mod\ 26)$, dengan *C* adalah indeks alfabet setelah pengenkripsian (akhir) dan *P* adalah indeks alfabet sebelum enkripsi (awal).

Berikut representasinya pada pesan "SAYA MAHASISWA INFORMATIKA", baik sebelum maupun setelah pengenkripsian.

Huruf (Indeks) awal	Huruf (Indeks) akhir
A(0)	D(3)
F(5)	I(8)
H(7)	K(10)
I(8)	L(11)
K(10)	N(13)
M(12)	P(15)
N(13)	Q(16)
O(14)	R(17)
R(17)	U(20)
S(18)	V(21)
T(19)	W(22)
W(22)	Z(25)
Y(24)	B(1)

Setelah dilakukan pengenkripsian terhadap tiap huruf pada pesan tersebut tersebut, pesan yang terbaca akan menjadi "VDBD PDKDVLVZD LQIRUPDWLND"

Kekongruenan $C \equiv (P + 3)\ (mod\ 26)$ dapat lebih digeneralisasikan terkait pergeseran huruf dan banyaknya jumlah karakter yang terdefinisi.

Misalkan *C* adalah indeks representatif terhadap karakter setelah pengenkripsian, *P* adalah indeks representatif terhadap karakter sebelum pengenkripsian, *N* adalah jumlah karakter terdefinisi yang mengandung karakter berindeks *P* dan *C*, serta *D* adalah besar pergesaran huruf yang diinginkan, maka untuk mengenkripsi/mendekripsi karakter berindeks *P* sejauh *D* sehingga menghasilkan karakter representatif berindeks *C* adalah sebagai berikut:

$$C \equiv (P \pm D)\ (mod\ N)$$

B. Kriptografi Kunci Publik RSA

Pada tahun 1976, Ronald Rivest, Adi Shamir, dan Leonard Adleman memperkenalkan sistem kunci publik yang memanfaatkan konsep teori bilangan. Sistem kunci publik tersebut dikenal dengan RSA.

Pada algoritma RSA, tiap pengguna memiliki sepasang tipe kunci dengan deskripsi sebagai berikut:

Tipe Kunci (notasi)	Kegunaan	Sifat
Publik (e)	Enkripsi pesan	Publik
Privat (p)	Dekripsi pesan	Privat (rahasia)

Tabel 3. Deskripsi sepasang tipe kunci pada RSA.

- Algoritma RSA

1. Pilih dua bilangan prima, misalkan *p* (rahasia) dan *q* (rahasia).
2. Hitung *n* = *pq* (tak-rahasia)
3. Hitung *m* = (*p*-1)(*q*-1) (rahasia)
4. Pilih sebuah bilangan bulat untuk kunci publik, misal *e*, yang relatif prima terhadap *m*, yaitu PBB(*m*, *e*) = 1.
5. Untuk mengenkripsi pesan maka:
   $p_t{}^e \equiv c(mod\ n) \Leftrightarrow c = p_t{}^e\ mod\ n$
   Dengan *c* adalah sub-bagian kode enkripsi yang terbentuk dan p_t adalah potongan beberapa karakter pada kode enkripsi atau representasi bilangan bulat dari karakter-karakter sebenarnya yang panjangnya tetap.

   Untuk mendekripsi pesan maka:
   $ed \equiv 1(mod\ m)$
   $c^d \equiv p_t(mod\ n) \Leftrightarrow p_t = c^d\ mod\ n$
   Dengan *d* merupakan kunci dekripsi.

Berikut merupakan kode enkripsi pada kata "MUDAH". Misalkan tiap karakter pada kata "MUDAH" direpresentasikan dengan kode ASCII sehingga menjadi 7785686572.

1. Misal, *p* = 59 dan *q* = 41
2. *n* = *pq* = 2419.
3. *m* = (*p*-1)(*q*-1) = 2320
4. Ambil *e* = 3 karena PBB(2320, 3) = 1.
5. Enkripsi:
   Misalkan p_t merepresentasikan potongan-potongan pada kode ASCII yang panjangnya 3 sehingga
   $p_{t_1} = 778$ $p_{t_3} = 657$
   $p_{t_2} = 568$ $p_{t_4} = 002$
   $c_1 = 778^3\ mod\ 2419 = 1803$
   $c_2 = 568^3\ mod\ 2419 = 1506$
   $c_3 = 657^3\ mod\ 2419 = 1928$
   $c_4 = 2^3\ mod\ 2419 = 8$

Sehingga kode enkripsi yang dihasilkan adalah 1803 1506 1928 8

Jika dilakukan pendekripsian terhadap kode enkripsi:
$3d \equiv 1(mod\ 2320) \Leftrightarrow d = 1547$

$p_{t_1} = 1992^{1547}\ mod\ 2419 = 778$
$p_{t_2} = 592^{1547}\ mod\ 2419 = 568$
$p_{t_3} = 1233^{1547}\ mod\ 2419 = 657$
$p_{t_4} = 8^{1547}\ mod\ 2419 = 2$

Terbentuk kode ASCII 7785686572 yang membentuk kata “MUDAH”.

IV. Simpulan

Salah satu kegunaan nyata dari konsep-konsep teori bilangan adalah pada bidang kriptografi, secara khusus pada Kriptografi Caesar Chiper dan Kriptografi Kunci-Publik RSA yang dibahas pada makalah ini. Konsep-konsep seperti kekongruenan, pembagi bersama terbesar dua bilangan, dan relatif prima sungguh berperan dalam perkembangan kriptografi yang sangatlah dibutuhkan kehadirannya oleh masyarakat modern.

Berdasarkan hasil pembahasan, Kriptografi Caesar Chiper relatif lebih mudah dan cepat dalam proses pengenkripsian suatu pesan dibandingkan Kriptografi Kunci-Publik RSA, namun dari segi keamanan relatif sangatlah rentan terdekripsi dibandingkan Kriptografi Kunci-Publik RSA.

V. Ucapan Terima Kasih

Alhamdulill$\bar{a}$h, atas seluruh nikmat yang diberikan-Nya Subh$\bar{a}$nahu Wata’$\bar{a}$la, akhirnya makalah ini dapat terselesaikan dengan baik dan tepat waktu. Penulis mengucapkan terima kasih kepada Dra. Harili M.Sc. selaku dosen K2 mata kuliah IF 2120 Matematika Diskrit atas segala bimbingannya, tenaganya, kesabarannya, dll. selama satu semester ini. Selain itu, penulis turut berterima kasih kepada Dr. Ir. Rinaldi Munir, M. T., atas segala bantuan “tak-langsungnya,” seperti penyedian situs dan bahan ajar yang diberikan. Penulis juga mengucapkan terima kasih kepada seluruh pihak yang, baik secara langsung maupun tidak langsung, telah membantu penulis dalam penyusunan makalah atau/dan khususnya selama satu semester perkuliahan ini.

Referensi

[1] Munir, Rinaldi. 2016. Matematika Diskrit Edisi Revisi keenam. Bandung: Informatika Bandung.

[2] *Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (PDF).*

[3] *Coppersmith, Don (1997). "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities" (PDF).*

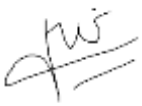
[4] https://www.ijarse.com/images/fullpdf/1483098559_N218ijarse.pdf diakses pada 11 Desember 2020.

[5] https://www.youtube.com/watch?v=0lOBubJRHSY diakses pada 11 Desember 2020.

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, 11 Desember 2020



Dwi Kalam Amal Tauhid - 13519210