Aplikasi Teori Bilangan Bulat Untuk Menjaga Keamanan Pesan Teks dengan Teknik Kriptografi

Syaiful Anwar - 13517139[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13517139@std.stei.itb.ac.id

***Abstrak*—Dalam berkomunikasi diperlukan keamanan pesan agar pelakunya mendapat rasa nyaman dalam berkomunikasi. Untuk menjaga keamanan pesan, sudah sejak lama manusia menggunakan teknik yang disebut Kriptografi. Dengan kriptografi diharapkan pesan dapat terjaga keamanannya hingga sampai kepada penerima pesan. Dalam kriptografi, pesan disandikan dengan proses enkripsi yang menggunakan suatu kunci tertentu. Hasil enkripsi pesan disebut *ciphertext*. Kemudian untuk membaca isi pesan, penerima juga harus melakukan proses pengembalian *ciphertext* menjadi pesan awal atau *plaintext* yaitu melalui proses dekripsi. Dalam proses dekripsi juga memerlukan suatu kunci tertentu. Kerena menyangkut keamanan, kriptografi juga memiliki kekuatan yang berbeda tiap tekniknya. Saat ini, kriptografi lebih menekankan kekuatan pada kunci ketimbang pada algoritmanya. Dalam hal inilah peran teori bilangan bulat penting dalam kriptografi. Teori bilangan bulat menjadi dasar dalam membentuk kompleksitas dari kunci yang dibuat. Kekuatan kriptografi yang didasarkan pada kuncinya lebih baik daripada kriptografi yang didasarkan pada kekuatan algoritmanya. Hal ini karena suatu kunci dapat memiliki jutaan bahkan miliaran kemungkinan sehingga mempersulit suatu *ciphertext* dapat dipecahkan dengan cepat.**

***Kata kunci*—Teori bilangan bulat, keamanan, pesan, kriptografi.**

I. PENDAHULUAN

Sebagai makhluk sosial, manusia tidak dapat dilepaskan dari komunikasi. Komunikasi antara dua orang atau lebih dapat dilakukan melalui berbagai cara yaitu dengan lisan, tulisan, isyarat, atau kombinasi dari ketiganya. Cara-cara tersebut dapat diimplementasikan dalam berbagai media seperti dialog langsung, percakapan melalui telepon, surat-menyurat, telegram, atau surat elektronik. Perkembangan zaman membuat manusia memiliki pilihan yang lebih beragam dalam melakukan komunikasi satu sama lain. Salah satu hal yang paling penting dalam berkomunikasi adalah ketersampaian pesan atau informasi dari pengirim kepada penerima.

Dalam berkomunikasi terkadang pesan yang hendak disampaikan bersifat rahasia atau hanya boleh diketahui oleh pengirim dan penerima pesan tersebut. Untuk itu, diperlukan suatu sistem yang dapat menjaga keamanan pesan tersebut hingga sampai ke penerima. Guna menjaga keamanan pesan pengirim dapat melakukan teknik kriptografi pada pesan sehingga dapat meningkatkan keamanan pesan tersebut.

Menurut sejarahnya, teknik kriptografi pertama digunakan oleh bangsa Mesir kuno sekitar 4000 tahun yang lalu yaitu *Hieroglyph*, kemudian Julius Caesar mengenalkan teknik kriptografi yang kemudian dikenal dengan *Caesar cipher*. Kriptografi juga digunakan pada masa perang dunia untuk mengantisipasi pesan bocor pada pihak lawan bila ada penyadapan oleh pihak lawan.

Pada mulanya kriptografi bersifat bebas yaitu setiap orang mempunyai caranya tersendiri dalam merahasiakan pesan. Seiring perkembangan zaman, kriptografi kemudian menjadi sebuah ilmu karena teknik-teknik kriptografi dapat dirumuskan secara matematik. Karena itulah kriptografi sangat erat hubungannya dengan teori bilangan bulat yang menjadi dasar dari teknik-teknik kriptografi.

Dalam makalah ini akan dijelaskan aplikasi dari teori bilangan bulat pada beberapa teknik kriptografi yang ada.

II. TEORI DASAR

A. Kriptografi

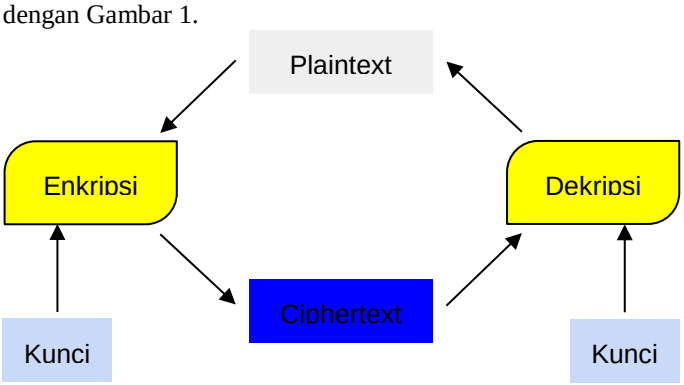
Kriptografi memiliki asal kata dari bahasa Yunani yaitu κρυπτός kryptós, dan γράφειν graphein. kryptós artinya tersembunyi, rahasia, dan γράφειν graphein artinya tulisan. Jadi kriptografi dapat diartikan menjadi "tulisan rahasia". Menurut Kamus Besar Bahasa Indonesia (KBBI),

> **Kriptografi** /krip·to·gra·fi/ (n) 1 (Linguistik) penyelidikan tentang kode rahasia; 2 teknik yang mengubah data menjadi berbeda dari aslinya dengan menggunakan algoritme matematika sehingga orang yang tidak mengetahui kuncinya tidak akan dapat membongkar data tersebut.

Dalam kriptografi, ada istilah yang sering dipakai yaitu enkripsi dan dekripsi. Enkripsi adalah proses pengubahan pesan dalam kode atau sandi, sedangkan dekripsi adalah proses pengembalian pesan yang sudah tersandikan ke pesan awal. Selain enkripsi dan dekripsi, dalam kriptografi juga terdapat istilah *plaintext* dan *ciphertext*. *Plaintext* adalah teks atau pesan awal yang hendak disandikan. *Ciphertext* adalah teks atau pesan yang telah tersandikan.

Untuk melakukan proses enkripsi dan dekripsi diperlukan

sebuah kunci. Dengan kunci tersebut pengirim dapat mengenkripsi *plaintext* menjadi *ciphertext* dan dengan kunci tersebut pula penerima dapat mendekripsi *ciphertext* menjadi *plaintext*. Skema dalam kriptografi dapat diperlihatkan sesuai dengan Gambar 1.



Gambar 1. Skema Kriptografi

Pada Gambar 2., memperlihatkan perbandingan antara *plaintext* yang diambil dari puisi karya Sapardi Djoko Damono dan *ciphertext* yang disandikan dengan suatu teknik kriptografi tertentu yang menggunakan kunci khusus dari *plaintext* tersebut.

aku ingin mencintaimu dengan sederhana
dengan kata yang tak sempat diucapkan
kayu kepada api yang menjadikannya abu

aku ingin mencintaimu dengan sederhana
dengan isyarat yang tak sempat disampaikan
awan kepada hujan yang menjadikannya tiada
sapardi djoko damono

(a)

nkv qygia gkecpatbqxu drhmrn zrdfzsann
xkegha kbbl yaaa zrk zrmqie dihwggkha
kbgf kecujr awv ybvr meadguirnnogl abh

uql iutio upncvhzrith dfvran fyjvronnb
lpngnh ojyheau glng guq jetcau ltsazjgzkha axiy
kecujr hbwao glng zytaakvkbvyya gcgua
znpbzoi dwiqf dhzoow

(b)

Gambar 2. (a) *plaintext* (b) *ciphertext*

Terlihat disini bahwa penggunaan kriptografi bukanlah agar komunikasi tidak diketahui sama sekali oleh orang lain, melainkan membuat pesan terjaga kerahasiaanya. Jadi walaupun komunikasi antara pengirim dan penerima dapat diketahui oleh orang lain melalui adanya *ciphertext*, tetapi isi pesannya hanya dapat diketahui oleh orang yang memiliki kunci untuk mendekripsikan *ciphertext* tersebut. Contoh nyatanya adalah saat pembaca hanya melihat *ciphertext* pada Gambar 2, pembaca tidak dapat memahami isi dari pesan tersebut, berbeda dengan penulis yang mempunyai kunci untuk melakukan dekripsi *ciphertext* tersebut.

Skema kriptografi pada Gambar 1, dapat pula dituliskan dalam notasi matematis. Jika P adalah *plaintext*, dan C adalah *ciphertext*, maka terdapat fungsi E sebagai fungsi enkripsi yaitu fungsi yang memetakan P ke C. Notasi matematisnya sebagai berikut.

$$E(P) = C$$

Dan terdapat pula fungsi D sebagai fungsi dekripsi yaitu fungsi yang memetakan C ke P. Notasi matematisnya sebagai berikut.

$$D(C) = P$$

karena enkripsi kemudian dekripsi mengembalikan *plaintext* ke *plaintext*, maka kesamaan berikut harus dapat dipenuhi.

$$(D \circ E)(P) = P$$

Untuk mendapat isi pesan sesuai yang diharapkan, proses dekripsi harus menggunakan kunci yang sesuai pada proses enkripsi. Disebutkan "menggunakan kunci yang sesuai" dan bukan "menggunakan kunci yang sama", karena tidak selalu kunci yang digunakan dalam proses enkripsi sama dengan kunci yang digunakan pada proses dekripsi. Hal ini berkaitan dengan pengelompokan kriptografi yaitu kriptografi kunci-simetri (*symmetric-key cryptography*) dan kriptografi kunci-nirsimetri (*asymmetric-key cryptography*) / kriptografi kunci-publik.

Pada kriptografi kunci-simetri, kunci yang digunakan pada proses enkripsi sama atau identik dengan kunci yang digunakan pada proses dekripsi. Contoh kriptografi kunci-simetri adalah *Caesar Cipher* dan *Vigenere Cipher*. Sedangkan pada kriptografi kunci-nirsimetri, kunci yang digunakan pada proses enkripsi adalah kunci publik dan kunci yang digunakan pada proses dekripsi adalah kunci privat. Contoh kriptografi kunci-nirsimetri adalah algoritma RSA (Rivest-Shamir-Adleman).

B. Hubungan Kriptografi dengan Teori Bilangan Bulat

Telah disebutkan bahwa skema kriptografi dapat dibuat dalam notasi matematis. Dalam notasi tersebut terdapat fungsi yang memetakan satu jenis teks ke teks yang lain. Dalam penerapannya, fungsi tersebut didasarkan pada teori bilangan bulat yang memuat,

- Bilangan bulat dan sifat-sifat pembagian;
- Algoritma *Euclidean;*
- Aritmetika modulo;
- Bilangan prima.

Algoritma *Euclidean* adalah algoritma yang dapat digunakan untuk mencari Pembagi Bersama Terbesar / PBB (*greatest common divisor*) dari dua buah bilangan bulat. Ditemukan oleh seorang matematikawan Yunani bernama Euclid yang kemudian menuliskan algoritma tersebut dalam buku karyanya yang berjudul *"Element"*.

Algoritma *Euclidean* dalam mencari PBB dirumuskan sebagai berikut.

Misalkan m dan n adalah bilangan bulat tak negatif

dengan $m \geq n$ serta $q_1,q_2,...,q_n$ adalah bilangan bulat. Misalkan $r_0 = m$ dan $r_1 = n$. Terapkan algoritma berulang,

$r_0 = r_1q_1 + r_2 \quad 0 \leq r_2 \leq r_1,$

$r_1 = r_2q_2 + r_3 \quad 0 \leq r_3 \leq r_2,$

.

.

.

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

$r_{n-1} = r_nq_n + 0$

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

Jadi, PBB dari m dan n adalah sisa pembagian terakhir yang tak nol atau sama dengan hasil bagi terakhir yang bersisa nol dari runtunan pembagian tersebut.

Selain algoritma *Euclidean,* Aritmetika modulo (*modular arithmethic*) mempunyai peran yang terbilang penting dalam kriptografi. Aritmetika modulo menggunakan operator khusus yaitu **modulo (mod)** . Operator modulo akan menghasilkan sisa pembagian jika digunakan pada pembagian bilangan bulat. Contoh, 26 dibagi 3 menghasilkan 8 dan sisa bagi 2, maka 26 mod 3 = 2 (dibaca "26 modulo 3"). Operator mod didefinisikan sebagai berikut,

Misalkan a dan m adalah bilangan bulat dan $m > 0$,
a mod m memberikan sisa pembagian apabila a dibagi m, atau a mod m = q sedemikian sehingga
$a = mp + q$, dengan $0 \leq q < m$.

Dalam aplikasinya, adapula teknik kriptografi yang memanfaatkan teori bilangan terkait bilangan prima. Bilangan prima adalah bilangan asli yang lebih besar dari 1, yang hanya memiliki faktor pembagi 1 dan bilangan itu sendiri. Itulah beberapa topik terkait teori bilangan yang diaplikasikan pada teknik kriptografi.

Penerapan teori bilangan pada kriptografi sangatlah penting, karena teknik kriptografi umumnya mengaplikasikan teori bilangan sebagai dasar algoritma dan kuncinya. Terlebih lagi saat ini algoritma kriptografi tak lagi menjadi kekuatan utama dari kriptografi modern. Namun, kriptografi modern lebih mengutamakan kekuatan kunci pada kriptografinya.

Kekuatan kriptrografi dapat dibedakan menjadi kekuatan algoritma dan kekuatan kunci. Dalam hal ini, algoritma kriptografi adalah fungsi matematika yang digunakan dalam proses enkripsi dan deskripsi. Kekuatan suatu algoritma kriptografi diukur dari jumlah proses yang dilakukan dalam proses memecahkan data *ciphertext* menjadi *plaintext*. Semakin banyak proses yang dilakukan, maka semakin kuat algoritma kriptografinya, yang berarti semakin aman untuk digunakan untuk menyandikan pesan, di sisi lain berarti semakin banyak waktu yang dibutuhkan dalam proses kriptografinya. Kekuatan kriptografi semacam ini ditentukan dengan menjaga kerahasiaan algoritmanya, maka algoritma kriptografi semacam ini disebut algoritma *restricted*. Algoritma *restricted* saat ini tidak cocok digunakan karena menjadi sangat rentan bocor, dapat dilihat pada contoh berikut. Misalkan sebuah tim mengirimkan pesan dengan terlebih dulu menyandikannya dengan sebuah algoritma khusus yang seragam. Misalkan algoritmanya adalah menempatkan karakter pertama setiap kata menjadi karakter terakhir lalu menambahkan imbuhan -erb sebagai akhiran. Contohnya,

Plaintext : CHICKEN DINNER
Ciphertext : HICKENCERB INNERDERB

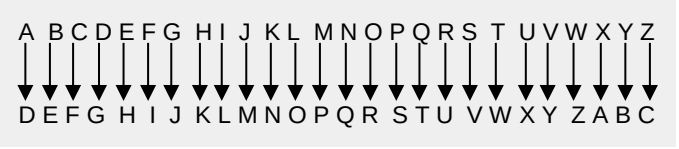
Digunakanlah kembali algoritma yang sama untuk mendeskripsikan pesan. Kerentanan algoritma *restricted* adalah apabila ada satu orang keluar dari tim, maka algoritma kriptografi pesan yang dipakai tadi harus diubah karena dikhawatirkan kerahasiaan algoritma tersebut dapat bocor oleh orang yang keluar tim tersebut. Oleh karena itu, kekuatan pada algoritma kriptografi tidak lagi menjadi dasar dari kekuatan kriptografi modern. Pada kriptografi modern, algoritma tidak lagi menjadi hal paling rahasia bahkan boleh saja diketahui publik. Yang paling dijaga kerahasiaannya adalah kunci kriptografinya. Sehingga kekuatan kriptografinya terletak pada kunci, yang berupa dereten karakter atau bilangan bulat. Proses enkripsi dan dekripsi hanya dapat dilakukan oleh orang yang mengetahui kunci tersebut. Karena itulah kriptografi sering menggunakan dasar teori bilangan bulat sebagai dasar algoritma dan juga kuncinya yang kemudian dapat meningkatkan kekuatan kunci tersebut.

III. KRIPTOGRAFI

Pada bagian ini akan dibahas beberapa contoh teknik kriptografi yang menjadi dasar dari pengembangan ilmu kriptografi saat ini. Tujuan dari mempelajari teknik-teknik tersebut adalah agar mendapat gambaran yang lebih jelas terkait kriptografi dan kaitannya dengan pengaplikasian teori bilangan bulat di dalamnya. Teknik-teknik yang akan dibahas merupakan contoh perkembangan yang terjadi pada ilmu kriptografi dari masa ke masa.

A. Caesar Cipher

Julius Caesar adalah orang yang mengenalkan teknik kriptografi ini. Karena itulah Teknik ini memiliki nama *Caesar* cipher. Pada masa Caesar, ia menggunakan teknik ini untuk menyandikan pesan yang ia kirim sebagai seorang kaisar kepada gubernurnya. Prinsip dasar dari *Caesar cipher* mengacu pada jenis kriptografi klasik yaitu Cipher substitusi. Pada *Caesar cipher*, setiap karakter huruf dalam pesan disubstitusi dengan huruf ketiga setelahnya dari susunan alfabet. Dalam hal ini kuncinya adalah jumlah pergeseran huruf yaitu 3 (tiap huruf digeser 3 ke kanan). Berikut adalah gambaran substitusi tiap huruf dalam alfabet dari *plaintext* ke *ciphertext.*



Gambar 3. Substitusi *plaintext* ke *ciphertext*

Jika setiap huruf alfabet dikodekan denganbilangan bulat dari 0 hingga 25, dengan, A = 0, B = 1, … , Z = 25, maka *Caesae*

cipher dapat dinotasikan secara matematis sebagai fungsi yang menyandikan plainteks P_i menjadi C_i dengan aturan sebagai berikut

$$E(P_i) = C_i = (P_i + 3) \ mod \ 26$$
$$D(P_i) = P_i = (C_i - 3) \ mod \ 26$$

P_i adalah karakter *plaintext* ke-I dan C_i adalah karakter *ciphertext* ke-i. E adalah fungsi enkripsi dan D adalah fungsi dekripsi.

Untuk nilai kunci k (jumlah pergeseran huruf sebanyak k), *Caesar cipher* dapat diformulasikan sebagai berikut.

$$E(P_i) = C_i = (P_i + k) \ mod \ 26$$
$$D(P_i) = P_i = (C_i - k) \ mod \ 26$$

k = nilai kunci, Pi adalah karakter plaintext ke-I dan Ci adalah karakter ciphertext ke-i. E adalah fungsi enkripsi dan D adalah fungsi dekripsi. Modulo 26 menandakan *Caesar cipher* yang diterapkan pada alfabet 26 karakter.

Dalam praktiknya, *Caesar cipher* biasa disajikan dalam kelompok n-karakter atau dengan menghilangkan spasi yang ada. Hal ini bertujuan menyulitkan usaha pembongkaran sandi. Misalkan sebuah *ciphertext* = PHUGHND DWDRH PDWL, maka dapat diubah menjadi,

Dikeompokkan 3-huruf : PHU GHN DDW DRH PDW L

Dihilangkan spasinya : PHUGHNDDWDRHPDWL

Caesar cipher juga dapat diterapkan pada karakter ASCII yang berjumlah 256, maka formulasinya menjadi,

Untuk 256 karakter ASCII, maka:

$$E(P_i) = C_i = (P_i + k) \ mod \ 256$$
$$D(P_i) = P_i = (C_i - k) \ mod \ 256$$

k = nilai kunci, Pi adalah karakter *plaintext* ke-i dan Ci adalah karakter *ciphertext* ke-i. E adalah fungsi enkripsi dan D adalah fungsi dekripsi. Modulo 256 menandakan *Caesar cipher* yang diterapkan pada ASCII 256 karakter.

Terlihat dari beberapa algoritma kriptografi di atas, bahwa teknik ini mempunyai kelemahan yaitu mudah dipesahkan karena memiliki kemungkinan kunci yang terbilang sedikit yaitu hanya 26 kunci pada alfabet. kuncinya sangat sedikit (hanya ada 26 kunci).

B. Vigènere Cipher

Vigènere Cipher petama kali dikenalkan oleh seorang diplomat dan kriptologis berkebangsaan Perancis pada tahun 1586, bernama Blaise de Vigènere. *Vigènere Cipher* pernah digunakan oleh pasukan Tentara Konfederasi (*Confederate Army*) pada Perang Sipil Amerika (*American Civil war*). Dalam melakukan enkripsi dengan menggunakan Teknik *Vigènere Cipher*, dipergunakan Bujursangkar *Vigènere* untuk memudahkan proses tersebut. Pada dasarnya, *Vigenere cipher* adalah adaptasi *Caesar cipher* yang menggunakan kunci sebuah frasa atau gabungan karakter dan bukan lagi hanya sebuah nilai bilangan bulat yang digunakan pada *Caesar cipher*. Bujursangkar *Vigenere* dapat dilihat pada Tabel 1. Dapat dilihat bahwa kolom mewakili *plaintext* dan baris mewakili kunci. Jika pada *Caesar cipher* huruf yang sama akan menghasilkan *ciphertext* yang sama, sedangkan pada *Vigenere cipher* huruf yang sama dapat menghasilkan *ciphertext* yang berbeda bergantung pada kunci yang digunakan untuk mengenkripsi *plaintext* tersebut. Pada *Vigenere* cipher, jika kuncinya lebih pendek daripada panjang *plaintext*, maka kunci tersebut diulang secara periodik sehingga Panjang kuncinya sama dengan Panjang *plaintext*.

Berikut ini contoh penggunaan Vigènere Cipher.
kunci = COCO
Plaintext : INI PLAINTEXT

Tabel 1. Bujursangkar *Vigenere*

Kunci \ Plaintext	**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

Kunci : COC OCOCOCOCO

Hasil enkripsi seluruhnya adalah sebagai berikut:

Ciphertext : KBK DNOKBVSZH

Terlihat bahwa hasil enkripsi huruf "T" adalah "V" jika dienkripsi dengan kunci "C" dan "H" jika dienkripsi dengan kunci "O". inilah yang membedakan *Vigenere cipher* dengan *Caesar cipher*. Dapat ditarik kesimpulan juga bahwa pada dasarnya, setiap enkripsi huruf dalam *Vigenere cipher* adalah enkripsi huruf dalam *Caesar cipher* dengan kunci yang berbeda-beda. Secara matematis untuk kasus enkripsi "T" dapat dinotasikan sebagai berikut.

$$E(\text{'T'}) = (\text{'T'} + \text{'C'}) \; mod \; 26 = \text{V}$$
$$E(\text{'T'}) = (\text{'T'} + \text{'O'}) \; mod \; 26 = \text{H}$$

Maka untuk notasi matematis dari *Vigenere cipher* akan sama dengan *Caesar cipher*, bedanya nilai kuncinya berbeda beda tiap karakternya.

Vigenere Cipher memiliki keunggulan dibandingkan *Caesar cipher* pada hasil enkripsi huruf yang sama tidak selalu menghasilkan huruf *ciphetext* yang sama pula. Akibatnya proses kriptanalisis pada *Vigenere cipher* akan lebih sulit jika tidak mengetahui kuncinya.

C. Algoritma RSA (Rivest-Shamir-Adleman)

Nama algoritma RSA didapat dari singkatan ketiga orang penemunya yaitu "R" dari kata Rivest yang diambil dari nama Ron Rivest, "S" dari kata Shamir yang diambil dari nama Adi Shamir, dan "A" dari kata Adleman yang diambil dari nama Len Adleman. Ketiganya merupakan peneliti yang berasal dari *Massachussets Institute of Technology* (MIT). Algoritma ini dikemukakan pada tahun 1976. Bilangan prima dan aritmatika modulo menjadi dasar dari proses enkripsi dan dekripsi yang dilakukan dalam algortima RSA. Kunci enkripsi dan kunci deskripsi algortima RSA merupakan bilangan bulat. Algortima RSA merupakan contoh kriptografi kunci-nirsimetri karen memanfaatkan kunci publik untuk kunci enkripsi dan kunci privat untuk kunci dekripsi. Kedua kunsi tersebut khusus dan berbeda. Kunci enkripsi bersifat publik dan tidak dirahasiakan sehingga dapat diketahui umum, namun kunci untuk deskripsi bersifat rahasia.

Kunci deskripsi didapatkan dari operasi matematika yang dilakukan pada beberapa buah bilangan prima bersama-sama dengan kunci enkripsi. Kunci enkripsi dapat diperoleh dengan memfaktorisasi sebuah bilangan non prima menjadi faktor primanya. Hal ini menjadi sulit apabila bilangan yang dicari faktor primanya bernilai besar, karena sampai saat ini belum ada algoritma efisien yang mampu memperoleh faktor prima dari suatu bilangan nonprima dalam pemfaktoran. Semakin besar bilangan non-primanya tentu akan semakin sulit menemukan faktor primanya. Algoritma RSA semakin kuat apabila semakin sulit untuk mendapatkan faktor prima dari bilangan nonprima tersebut.

Pada dasarnya algoritma RSA cukup sederhana. Algortima ini secara ringkas dapat dinyatakan dalam langkah-langkah sebagai berikut.

1. *Pilih dua buah bilangan prima sembarang, misal a dan b. Kemudian jaga kerahasiaan kedua bilangan tersebut.*
2. *Lalu hitung*
   $n = a \times b$.
   nilai n tidak dirahasiakan.
3. *Kemudian hitung*
   $m = (a - 1) \times (b - 1)$.
   Saat m telah dihitung, a dan b dapat dihilangkan untuk mencegah bocor pihak lain.
4. *Lalu pilih sebuah bilangan bulat untuk kunci publik, misal e, yang relatif prima terhadap m*
5. *Untuk medapat kunci dekripsi, missal d, diperoleh dengan kekongruenan*
   $ed \equiv 1 \; (mod \; m)$.
   kemudian lakukan enkripsi terhadap isi pesan dengan persamaan
   $E(pi) = ci = pie \; mod \; n$,
   yang dalam hal ini pi adalah blok plainteks, ci adalah chiperteks yang diperoleh, dan e adalah kunci enkripsi (kunci publik). Harus dipenuhi persyaratan bahwa nilai pi harus terletak dalam himpunan nilai 0, 1, 2, …, n – 1 untuk menjamin hasil perhitungan tidak berada di luar himpunan.
6. *Proses deskripsi dilakukan dengan menggunakan persamaan*
   $D(ci) = pi = cid \; mod \; n$,
   yang dalam hal ini d adalah kunci deskripsi.

Pehatikan bahwa dalam langkah 4 kekongruenan

$ed \equiv 1 \; (mod \; m)$

sama dengan

$ed \; mod \; m = 1$.

ed mod m = 1 ekivalen dengan ed = km + 1 sehingga akan menghasilkan persamaan

$d = (1 + km) / e$

akan terdapat bilangan bulat k yang menyebabkan persaman diatas memberikan bilangan bulat d.

Seperti yang telah diungkapkam di atas, kekuatan dan keamanan RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non-prima menjadi faktor primanya, yang dalam hal ini n = a × b. Saat n berhasil difaktorkan menjadi a dan b maka m = (a – 1) × (b – 1) dapat dihitung. Selanjutnya, karena kunci enkripsi e diumumkan (tidak rahasia), maka kunci deskripsi d dapat dihitung dari persamaan $e \times d \equiv 1 \; (mod \; m)$. Hal ini berbahaya karena artinya proses deskripsi dapat dilakukan oleh orang yang tidak berhak. Para penemu algortima RSA menyarankan nilai a dan b yang dipakai panjangnya lebih dari 100 digit. dengan demikian hasil kali n = a × b akan berukuran lebih dari 200 digit. Dengan begitu maka usaha yang diperlukan untuk melakukan pemfaktoran nilai n yang merupakan bilangan bulat 200 digit akan sangat besar sehingga kemungkinan isi pesan dapat terbongkar akan semakin kecil. Menurut keterangan para penemunya, dibutuhkan waktu komputasi 4 miliar tahun untuk mendapatka faktor prima bilangan yang memiliki 200 digit. (Dengan asumsi bahwa algoritma pemfaktoran yang digunakan adalah algoritma tercepat saat ini dan komputer yang dipakai mempunyai kecepatan 1 milidetik). Kekuatan dari algoritma ini adalah hasil dari belum ditemukannya algoritma yang efisien untuk

memfaktorkan bilangan-bilangan besar. Karena hal inilah membuat algorima RSA masih tetap dipakai hingga saat ini. Algoritma RSA masih direkomendasikan dalam melakukan penyandian pesan selagi belum ditemukan algoritma yang efisien untuk mendapat faktor prima dari sebuah bilangan bulat pada proses pemfaktoran.

IV. SIMPULAN

Dari ulasan di atas, kita dapat menyimpulkan bahwa dalam ilmu kriptografi sangat memerlukan dasar matematika diskrit terutama terkait teori bilangan bulat. Karena itu, dengan mempelajari ilmu tersebut, setidaknya kita dapat mengetahui pengaplikasian ilmu tersebut dalam kehidupan sehari-hari, terlebih kriptografi saat ini tak hanya menjadi ilmu untuk berkirim pesan rahasia saja melainkan sudah merambah ke ranah yang lebih luas yaitu keamanan data. Data-data pribadi seperti PIN ATM, informasi akun media social, hingga perpesanan pada aplikasi *chatting* telah menerepkan kriptografi agar privasi pengguna lebih terjaga dan keamanannya lebih terjamin. Dengan mengetahui ilmu kriptografi, kita dapat sadar betapa rentannya data kita sekaligus waspada pada saat menuliskan data pribadi di sebuah media.

Dan perlu diingat pula pada dasarnya tidak ada kriptografi yang benar-benar aman karena seiring berkembangnya zaman memungkinkan ditemukannya algoritma yang mampu memecahkannya.

REFERENSI

[1] Kamus Besar Bahasa Indonesia versi daring https://kbbi.web.id/kriptografi Diakses tanggal 8 Desember 2018, pukul 02.15 WIB

[2] Munir, Rinaldi. Bahan Ajar Mata Kuliah IF2120 Matematika Diskrit, Program Studi Teknik Informatika, Institut Teknologi Bandung. Bandung.

[3] Munir, Rinaldi. Bahan Ajar Mata Kuliah IF4020 Kriptografi, Program Studi Teknik Informatika, Institut Teknologi Bandung. Bandung.

[4] Wicaksono, Kukuh Nasrul. *Penerapan Teori Bilangan Bulat dalam Kriptografi dan Aplikasinya dalam Kehidupan Sehari-hari*, 2006. Bandung.

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, 9 Desember 2018

Syaiful Anwar
13517139