Penerapan Teori Bilangan pada Alat Token *Online Banking*

Radiyya Dwisaputra/13515023
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13515023@std.stei.itb.ac.id
radiyyasaputra@gmail.com

***Abstrak*—Teori Bilangan merupakan suatu dasar dari matematika. Teori bilangan terdiri dari berbagai hal mulai dari bilangan, phytagoras,dll. Salah satu materi dari teori bilangan ialah modulo atau keterbagian. Modulo dapat dikembangkan menjadi berbagai hal di kehidupan nyata. Pengembangan modulo diantara ialah enkripsi. Enkripsi digunakan untuk mengamankan suatu data yang dikirim. Enkripsi dibutuhkan agar pesan yang rahasia tidak bisa dipahami oleh orang lain kecuali penerima pesan. Pada makalah ini akan dibahas penerapan teori bilangan pada transaksi online banking.**

***Kata kunci*—enkripsi, online banking, alat token, modulo**

I. PENDAHULUAN

Semakin berkembangnya teknologi, berbagai sektor turut mengikuti perkembangan. Salah satu sektor tersebut ialah perbankan. Layanan bank mengalami peningkatan yang cukup pesat mulai dari layanan langsung, sms banking hingga *online banking*. Pelayanan yang semakin mudah membuat nasabah tidak perlu melakukan banyak usaha untuk melakukan sebuah transaksi. Salah satu alat yang dibutuhkan untuk melakukan *online banking* ialah Alat token.

Alat token *online banking* digunakan untuk mengamankan berbagai transaksi oleh nasabah bank yang dilakukan secara online. Pada umumnya pada bank di Indonesia, bagi nasabah yang menginginkan untuk menggunakan layanan *online banking* maka akan diberi sebuah alat yang berfungsi untuk memunculkan token secara random untuk mengamankan *online banking* yang dilakukan baik alat tersebut tersambung pada server bank ataupun tidak tersambung secara langsung oleh server bank. Pada *online banking* dilakukan metode autentikasi yang bermacam-macam, kegunaan alat token ialah untuk melakukan 2 faktor autentikasi yakni PIN, dan token.

Penelitian *online banking* pertama kali dilakukan pada tahun 1980 yang dilakukan oleh Bank-bank di Amerika dan Eropa. *Online banking* pertama kali mulai diperkenalkan kepada masyarakat di Amerika pada Oktober 1994 oleh *Stanford Federal Credit Union*. Di Indonesia, *online banking* diperkenalkan pertama kali oleh Bank Central Asia (BCA) pada tahun 2001. [2]

Pengenalan internet banking pun disertai dengan pemberian alat token untuk memberi kenayamanan dan keamanan para nasabah. Dari 2001 hingga sekarang sudah hampir semua bank di Indonesia menyediakan layanan *online banking*.

Online banking memiliki banyak manfaat dan kegunaan tetapi *online banking* juga memiliki beberapa kelemahan yang ada.

Manfaat menggunakan *online banking* :

1. Mudah dan dapat dilakukan dimana saja
2. Melakukan transaksi non tunai / tidak perlu membawa uang
3. Mudah mencari info tentang kurs mata uang
4. Menghemat transportasi
5. Dapat mengetahui transaksi terakhir

Kelemahan menggunakan *online banking* :

1. Hanya bisa dilakukan dengan koneksi internet
2. Harus membawa alat token
3. Harus diakses melalui komputer/laptop atau handphone
4. Butuh keamanan lebih

Alat token yang beredar memiliki 2 jenis yakni alat token yang terhubung dengan server bank ataupun alat token yang tidak terhubung ke server bank. Kedua Alat bertujuan untuk menjaga keamanan transaksi *online banking* nasabah. [1]

Walaupun demikian keamanan internet banking juga perlu dilakukan oleh nasabah sendiri yaitu seperti halnya tidak melakukan *online banking* di komputer publik, tidak menggunakan *online banking* pada komputer/laptop yang mengandung malware karena malware tersebut bisa saja membaca pin nasabah tersebut sehingga pembuat malware dapat bertransaksi menggunakan rekening nasabah.

II. TEORI BILANGAN

Teori Bilangan merupakan ilmu yang ditemukan dari waktu yang sangat lama oleh bangsa-bangsa terdahulu seperti halnya oleh Suku Babilonia pada sekitar 7000SM yang memiliki lempengan yang memberikan hampiran $\sqrt{2}$ dan memiliki keakuratan hingga lima tempat desimal. Teori Bilangan memiliki perkembangan secara terus menerus, pada awalnya semua bilangan masih dilambangkan dengan benta tertentu seperti batu, kerikil,

tongkat, lempengan. Teori bilangan tidak hanya berkembang pada Suku Babilonia melainkan juga berkembang di suku lain. Simbol bilangan yang masih digunakan hingga saat ini ialah simbol bilangan yang digunakan oleh Bangsa Romawi. Seiring berjalan nya waktu mulai ditemukan berbagai teorema. Teorema phytagoras ditemukan sekitar 500 SM oleh matematikawan yang bernama Phytagoras.[3] Banyak tokoh- tokoh yang juga menemukan teorema-teorema dalam teori bilangan.

Pada zaman modern ini, Penggunaan Teori Bilangan sangat beragam bahkan materi teori bilangan modulo atau keterbagian diterapkan untuk menjaga keamanan sebuah sistem atau jaringan komputer.

Modulo merupakan pembagian bersisa sebuah bilangan yang biasanya bisa dituliskan seperti dibawah ini

$$A \bmod C = B$$

atau

$$A \equiv B \ (mod\ C)$$

Relasi kongruensi diatas memili arti

$$A = C * K + B$$

A,B, C dan K ialah sebuah bilangan bulat. Sehingga dapat diartikan bahwa A bila dibagi oleh C akan bersisa B.

Penggunaan modulo yang lebih luas ialah enkripsi. Contoh algoritma enkripsi sederhana ialah Chaesar Cipher yang ditemukan pada zaman Julius Caesar yakni dengan menggunakan prinsip modulo ialah menggeser huruf alfabet ke 3 kanan nya yang mana dalam kasus ini modulo yang digunakan ialah dengan pembagi 26 karena terdapat 26 huruf alfabet.

AKU BUKA WEB KAYU
menjadi
DNX EXND ZHE NDBX

Table 1

Konversi huruf ke kode huruf

Huruf	Kode
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

Penghitungan yang dilakukan yaitu mengubah huruf menjadi kode angka yakni A=0, B=1, C=2, dan seterusnya seperti pada tabel 1. lalu menggeser huruf dengan menggunakan penambahan pada kode angka lalu di modulo 26 yang berfungsi agar huruf tidak keluar dari kode huruf yang ada. Enkripsi ini digunakan agar pesan yang ingin disampaikan tidak dapat dibaca oleh orang lain, yang bermaksud untuk mengirimkan pesan rahasia pada zaman dahuu.

Algoritma Enkripsi yang lebih rumit ialah algoritma RSA. Algoritma RSA dibuat oleh Ron Rivest, Adi Shamir, dan Len Adleman yang ketiganya merupakan peneliti dari Massachussets Institute of Technology (MIT). Algoritma RSA ini terdapat 2 kunci yakni kunci privat dan kunci publik. Kunci publik digunakan untuk mengubah pesan biasa menjadi pesan terenkripsi dan bersifat bebas sedangkan kunci privat digunakan untuk mendeskripsi pesan sehingga bisa dibaca sebagai pesan normal, kunci privat ini hanya dimiliki oleh pembaca pesan saja. Perkembangan algoritma RSA di zaman modern ini cukup cepat, kunci RSA yang digunakan saat ini sebesar 1024 atau 2048 bit. Algoritma RSA sebagai berikut

Algoritma pembangkitan pasangan kunci

1. Pilih dua bilangan prima, p dan q (rahasia)
2. Hitung n = p*q. Besaran n tidak perlu dirahasiakan.
3. Hitung m = (p – 1)*(q – 1).
4. Pilih sebuah bilangan bulat untuk kunci publik, e, relatif prima terhadap m.
5. Hitung kunci dekripsi, d, melalui kekongruenan ed ≡ 1 (mod m). [6]

Secara pseudocode dapat ditulis dengan contoh berikut

```
Select the prime integers q=11, q=3.
n=pq=33; ϕ(n)=(p-1)(q-1)=20
Choose e=3
    Check gcd(3,20)=1
Compute d=7
    (3)d ≡ 1 (mod 20) [5]
```

Algoritma enkripsi dan dekripsi

Enkripsi :

$$c_i = p_i^{\,e} \ mod\ n$$

Dekripsi :

$$p_i = c_i^{\,d} \ mod\ n$$ [6]

Pembangkit bilangan acak merupakan sebuah penerapan modulo. Pembangkit bilangan acak merupakan pembentukan suatu bilangan acak dengan menggunakan

algoritma tertentu. Modulo dimanfaatkan untuk memperoleh rentang nilai, seperti halnya bilangan acak yang ingin diperoleh mulai dari 0 hingga 13 maka bilangan pembagi yang digunakan dalam modulo ialah 14. Bilangan yang dihasilkan tidak memiliki pola pola tertentu yang berarti bilangan benar-benar acak dalam rentang yang diinginkan.

Table 2

Pembangkit Bilangan Acak

N	X_N
0	0
1	2
2	1
3	5

$$X_N \equiv (X_{N-1} * 3 + 2)\ (mod\ 7)$$
$$X_N \equiv (X_{N-1} * 3 + 2)\ (mod\ 7)$$
$$X_N \equiv (X_{N-1} * 3 + 2)\ (mod\ 7)$$
$$X_N \equiv (X_{N-1} * 3 + 2)\ (mod\ 7)$$

III. CARA KERJA ALAT TOKEN

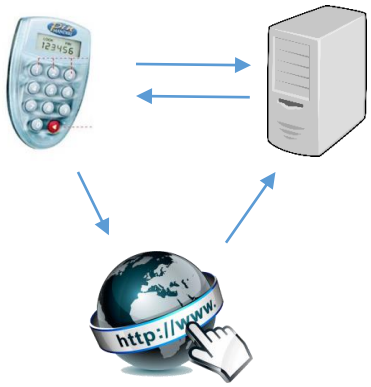
Dalam mengautentikasi seseorang terdapat 3 hal yang dapat digunakan

a. *Something that user knows*
   Sesuatu yang diketahui oleh pengguna seperti tanggal lahir, PIN, pertanyaan rahasia, dll.
b. *Something that user has*
   Sesuatu yang dimiliki oleh pengguna seperti sidik jari, retina mata, dll.
c. *Something that user is*
   Siapa pengguna tersebut. [1]

Alat token *online banking* merupakan alat untuk autentikasi sebuah nasabah bank, alat ini memiliki bentuk seperti kalkulator mini yang memiliki tombol-tombol angka yang berfungsi untuk memasukkan generator key dari internet dan juga akan menampilkan token pengguna untuk dimasukkan ke internet. Alat token *online banking* yang dimiliki oleh suatu nasabah dengan nasabah lain memiliki peraturan berbeda agar nasabah tidak bisa menggunakan token yang muncul pada nasabah lain.

Enkripsi pada alat token dilakukan agar *online banking* menjadi aman dan tidak bisa diretas. Enkripsi dilakukan dengan rumit dan tidak diketahui oleh manapun, bahkan nasabah bank pun tidak dapat mengetahui enkripsi apa yang digunakan untuk mendapatkan token pada alat token yang dimiliki hal ini bertujuan untuk menjaga keamanan agar tidak merugikan bank maupun nasabah-nasabah yang ada. Terdapat 2 macam alat token yang digunakan dalam *online banking* yaitu alat token yang tersambung ke server bank ataupun yang tidak. Kedua alat token ini memiliki kinerja yang berbeda. Walaupun demikian kedua token ini memiliki tujuan yang sama yaitu untuk menampilkan token verifikasi untuk transaksi tanpa diketahui oleh orang lain kecuali pengguna.

Pada alat token yang tersambung pada server bank, kinerja dengan algoritma RSA, Pada saat pengguna merequest token maka server bank akan mengirimkan sebuah kode yang telah di enkripsi dengan *public key* lalu kode tersebut di dekripsi oleh alat token. Setelah itu pengguna dapat memasukkan token sebagai verifikasi yang akan dikirimkan ke server bank kembali dengan *public key* yang berbeda lalu di dekripsi oleh server bank dengan *public key* untuk mengetahui apakah benar atau tidak token verifikasi yang telah dimasukkan. Mode ini disebut sebagai Mode Challenge/Response (C/R) yang berarti terjadi request kepada server dan pengiriman token dari server ke alat token.



Gambar 1 Cara kerja alat token terhubung dengan server.

http://2.bp.blogspot.com/-9ex5ubWxx24/UQSlQYmC6CI/AAAAAAAABNg/oG9JhC2LRtA/s1600/token+pin+mandiri.jpg

Pada alat token yang tidak tersambung oleh server, kinerja nya ialah dengan memasukkan algoritma pembangkit bilangan acak yang sama pada alat token dan server. Yang mana token sudah dirancang akan berubah dalam waktu tertentu. Antara alat token dan server memiliki setting waktu awal yang sama, sehingga nilai token tidak mungkin berbeda diantara server maupun alat token. Mode ini disebut sebagai Mode Self Generated yang mana alat token dan server masing-masing menggenerate token yang sama secara periodik.

Gambar 2 Cara kerja alat token tidak terhubung dengan server.

http://2.bp.blogspot.com/-9ex5ubWxx24/UQSlQYmC6CI/AAAAAAAABNg/oG9JhC2LRtA/s1600/token+pin+mandiri.jpg

Pengamanan dilakukan dengan enkripsi yang rumit dan juga One Time Password (OTP) yang berarti token hanya dapat digunakan satu kali saja. Sehingga setelah token diinput maka token pada server akan dihapus. OTP digunakan untuk mencegah adanya peretasan pada sistem.[4]

Penggunaan token membutuhkan waktu proses yang lebih cepat karena agar membuat data nasabah aman oleh karena itu perlu dilakukan adanya optimasi pada penggunaan algoritma RSA agar tidak menggunakan terlalu banyak memori karena pemrosesan angka yang terlalu besar.

$$c_i = {p_i}^e \bmod n$$

Penghitungan diatas dapat dioptimalkan dengan membagi pengerjaan agar nilai bilangan yang di modulo tidak terlalu besar yaitu

$$c_i = p_i \bmod n * {p_i}^{e-1} \bmod n$$
$$c_i = {p_i}^2 \bmod n * {p_i}^{e-2} \bmod n$$
$$c_i = {p_i}^3 \bmod n * {p_i}^{e-3} \bmod n$$
$$\vdots$$
$$c_i = {p_i}^e \bmod n$$

Hal serupa juga dilakukan pada algoritma dekripsi

$$p_i = {c_i}^d \bmod n$$

Dalam pengamanan alat token lainnya ialah dengan memaksimalkan kesalahan input pengguna yaitu sebanyak 3 kali hal ini berguna mencegah cara bruteforce yang berniat untuk menggunakan internet banking orang lain.

IV. PENGGUNAAN *ONLINE BANKING*

Pertama nasabah bank membuka situs untuk melakukan transaksi *online banking*, lalu nasabah bank akan diminta untuk memasukkan user id dan PIN.

Selain pada alat token, enkripsi juga diterapkan pada user id dan PIN nasabah bank, prinsip yang digunakan sama dengan alat token hanya saja untuk user id dan PIN sudah diketahui oleh nasabah sehingga tidak perlu membawa alat seperti alat token.

Perlu diperiksa keadaan komputer/piranti terlebih dahulu untuk terbebas dari virus, malware, worm karena dapat menyebabkan data nasabah dapat terekam melalui virus, malware atau worm. Dan juga perlu diperhatikan bahwa situs yang dituju benar karena bisa saja terdapat beberapa situs yang menampilkan display yang mirip agar ada orang yang mengira bahwa itu situs resmi.

Setelah nasabah memasukkan user id dan PIN, nasabah akan memilih transaksi yang ingin dan lakukan. Pada saat iniliah token yang ditampilkan pada alat token akan diminta.

Gambar 3 Tampilan awal Online Banking BCA

https://ibank.klikbca.com/

Gambar 4 Menu transfer pada Online Banking BCA

http://2.bp.blogspot.com/-zpKpzW8keNg/U7iVKm8DvBI/AAAAAAAAIlE/-6_Pbly9WGQ/s1600/cara+transfer+uang+melalui+internet+banking+bca+sesama+bca1.jpg

V. KESIMPULAN

Penerapan teori bilangan sangat luas, terutama di bidang enkripsi untuk keamanan sebuah data. Hal ini sangat penting dikarenakan banyak data yang tidak dapat diketahui oleh semua orang seperti data perusahaan, data tempat tinggal seseorang. Enkripsi sangat berguna untuk mengembangkan keamanan sebuah sistem (*cyber security)*. Teori bilangan dapat diterapkan untuk pengembangan teknologi yang sudah ada maupun penemuan teknologi yang akan datang.

VI. UCAPAN TERIMA KASIH

Terima kasih Penulis ucapkan kepada Allah SWT, karena atas karuniaNya makalah ini dapat diselesaikan untuk memenuhi tugas mata kuliah Matematika Diskrit IF2120. Penulis juga mengucapkan terima kasih sebesar-besarnya kepada Bapak Ibu Dosen yang telah memberikan ilmu yang bermanfaat untuk menyelesaikan makalah ini. Selain itu, penulis mengucapkan terima kasih kepada orang tua penulis dan teman-teman yang telah mendukung sehingga makalah ini dapat diselesaikan.

REFERENSI

[1] http://www.ilmuhacking.com/web-security/memahami-cara-kerja-token-internet-banking/ diakses pada 08 Desember 2016 pukul 20.00

[2] https://tonnymarezco.wordpress.com/2014/04/17/sejarah-internet-banking/ diakses pada 08 Desember 2016 pukul 19.00

[3] http://ku-mathitung.blogspot.co.id/p/sejarah-teori-bilangan.html diakses pada 08 Desember 2016 pukul 19.30

[4] http://www.explainthatstuff.com/how-security-tokens-work.html diakses pada 08 Desember 2016 pukul 20.15

[5] http://crypto.stackexchange.com/questions/15864/pseudocode-for-constant-time-modular-exponentiation diakses pada 08 Desember 2016 pukul 21.00

[6] Munir, Rinaldi. 2003. *Matematika Diskrit Edisi Kedua*. Bandung: Penerbit 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, 8 Desember 2016

Radiyya Dwisaputra -13515023