Aplikasi Teori Bilangan (Kriptografi) dalam Keamanan Transaksi dengan Mesin ATM

Nabila Hannania / 13519097
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13519097@std.stei.itb.ac.id

***Abstract*— *Automated Teller Machine* atau yang biasa disingkat dengan ATM adalah sebuah alat elektronik yang melayani nasabah bank untuk mengambil uang dan mengecek rekening tabungan mereka tanpa perlu dilayani oleh seorang "teller" manusia. Dalam melakukan transaksi dengan ATM nasabah diharuskan untuk memasukkan PIN sebelum melakukan transaksi, untuk memverifikasi kartu yang dimasukkan oleh nasabah di ATM. Hal ini untuk mencegah kartu nasabah digunakan oleh orang yang tidak bertanggungjawab. Proses verifikasi ini dilakukan di komputer pusat (host) bank, oleh karena itu harus ada komunikasi dua arah antara ATM dan komputer host. Selama prose transmisi dari ATM ke komputer host, PIN harus dilindungi dari penyadapan oleh orang yang tidak bertanggung jawab. Maka dari itu dalam transaksi menggunakan mesin ATM terdapat suatu sistem keamanan ATM. Yang mana sistem keamanan ini akan melindungi data yang dimasukkan selama transmisi adalah dengan mengenkripsikan PIN. Selain itu, PIN yang disimpan di dalam basisdata pada bank juga dienkripsi agar tidak dapat diketahui orang lain.**

***Keywords*—ATM, transaksi, PIN, enkripsi.**

I. PENDAHULUAN

Pada zaman sekarang, rata - rata orang menyimpan uang mereka di Bank. Selain dinilai lebih aman, menyimpan uang di Bank di nilai lebih efektif dan banyak keuntungan yang didapat. Dulu ketika kita ingin mengambil uang di rekening, ataupun melakukan transaksi lainnya kita harus pergi ke Bank. Proses dalam melakukan transaksinya pun cukup lama karena kita diharuskan mengisi beberapa berkas terlebih dahulu, kemudian mengantri sambil menunggu giliran kita. Proses ini tentu saja memakan banyak waktu, apalagi jika keadaan di Bank sedang ramai.

Namun sekarang, sudah ada yang namanya Mesin ATM, yang memungkinkan nasabah untuk melakukan transaksi yang biasa di lakukan di Bank pada mesin ATM, seperti penarikan uang tunai, mengirimkan uang, dan membayar tagihan. Hal ini tentu saja sangat menguntungkan bagi nasabah yang ingin melakukan transaksi dengan cepat. Selain itu, mesin ATM itu beroperasi selama 24 jam *nonstop*, sehingga para nasabah dapat melakukan transaksi kapan saja mereka luang. Tidak seperti transaksi di bank yang memiliki jam operasi tertentu.

Akan tetapi, dibalik keuntungannya terdapat juga kerugian dari melakukkan transaksi melalui mesin ATM, yaitu adanya kemungkinan terjadi penyadapan terhadap data yang kita masukkan ke mesin ATM yang berakibat orang lain dapat mengakses rekening kita.

Untuk mengatasi hal ini, mesin ATM memiliki suatu sistem keamanan yang dapat menjaga keamanan data nasabah. Sistem keamanan ini memanfaatkan konsep Teori Bilangan yang ada pada Kriptografi. Adapun yang dilakukan adalah mengenkripsi data nasabah menggunakan algoritma DES agar data tersebut tidak dapat dibaca oleh pihak lain yang tidak bertanggung jawab.

Pada makalah ini, penulis akan membahas mengenai Teori Bilangan dan aplikasinya pada Kriptografi yang mana nantinya prinsip - prinsip yang telah dijelaskan akan digunakan dalam sistem keamanan transaksi dengan mesin ATM. Pada makalah ini, penulis juga akan menjelaskan sedikit teantang cara kerja transaksi dengan mesin ATM dan bagaimana proses enkripsi data pada saat melakukan transaksi dengan mesin ATM.

II. LANDASAN TEORI

A. Teori Bilangan

Teori bilangan adalah cabang matematika murni yang ditujukan untuk mempelajari bilangan bulat (integer) atau fungsi bernilai bilangan bulat. Pegertian dari bilangan bulat (integer) itu sendiri adalah bilangan yang tidak mempunyai pecahan desimal. Contoh dari bilangan bulat antaar lain 8, 21, 8765, -34, 0, dsb. Selain bilangan bulat juga terdapat yang namanya bilangan riil. Berlawanan dengan bilangan bulat adalah bilangan riil yang mempunyai titik desimal. Contoh dari bilangan riil antara lain 8.0, 34.25, 0.02, dsb.

- Sifat Pembagian pada Bilangan Bulat

Misalkan terdapat 2 buah bilangan bulat yaitu, a dan b, dengan a > 0. a dikatakanj habis membagi b (a divides b) jika terdapat bilangan bulat c sedemikian sehingga b = ac.

Pernyataan diatas dapat dinotasikan sebagai : a | b jika b = ac, dengan c adalah bilangan bulat dan a > 0.

Contohnya terdapat dua buah bilangan bulat yaitu 4 dan 12, maka kedua bilangn bulat ini dapat dinotasikan sebagai 4 | 12 karena 12/4 = 3 (bilangan bulat) atau 12 = 4 * 3.

- Teorema Euclidean

Teorema Euclidean ini menjelaskan misalkan terdapat dua buah bilangan bulat, yaitu m dan n, dengan n > 0. Jika m dibagi dengan n maka hasil pembagiannya adalah q (quotient) dan sisanya r (remainder), sedemikian sehingga

$$m = nq + r$$

dengan $0 \leq r < n$.

❖ Pembagi Bersama Terbesar (PBB)

Misalkan a dan b bilangan bulat tidak nol. Pembagi bersama terbesar (PBB – greatest common divisor atau gcd) dari a dan b adalah bilangan bulat terbesar d sedemikian hingga d | a dan d | b. Dalam hal ini kita nyatakan bahwa PBB(a, b) = d.

Misalkan m dan n bilangan bulat, dengan syarat n > 0 sedemikian sehingga

$$m = nq + r \text{ , } 0 \quad r < n$$

maka PBB(m, n) = PBB(n, r)

❖ Algoritma Euclidean

Algoritma Euclidean bertujuan untuk mencari PBB dari dua buah bilangan bulat. Algoritma Euclidean ini sendiri ditemukan oleh Euclides, seorang matematikawan Yunani yang menuliskan algoritmanya tersebut dalam buku, Element.

Pada Algoritma Euclidean ini dijelaskan bila terdapat dua buah bilangan bulat tak negatif, yaitu m dan n dengan $m \geq n$. Kemudian, misalkan $r_0 = m$ dan $r_1 = n$. Lakukan secara berturut-turut pembagian untuk memperoleh

$r_0 = r_1q_1 + r_2$ $\quad 0 \leq r_2 \leq r_1$,
$r1 = r2q2 + r3$ $\quad 0 \leq r_3 \leq r_2$,
$r_{n-2} = r_{n-1}\, q_{n-1} + rn$ $\quad 0 \leq r_n \leq r_{n-1}$,
$r_{n-1} = r_nq_n + 0$

Berdasarkan pengertian PBB,
$PBB(m, n) = PBB(r_0 , r_1) = PBB(r_1, r_2) = \ldots =$
$PBB(r_{n-2}, r_{n-1}) = PBB(r_{n-1}, r_n) = PBB(r_n , 0) = r_n$

Jadi, PBB dari m dan n adalah sisa terakhir yang tidak nol dari runtunan pembagian tersebut

Diberikan dua buah bilangan bulat tak-negatif m dan n ($m \geq n$). Algoritma Euclidean berikut mencari pembagi bersama terbesar dari m dan n.

1. Jika n = 0 maka m adalah PBB(m, n); stop. tetapi jika $n \geq 0$, lanjutkan ke langkah 2.
2. Bagilah m dengan n dan misalkan r adalah sisanya.
3. Ganti nilai $_n$ dengan nilai n dan nilai n dengan nilai r, lalu ulang kembali ke langkah 1.

❖ Kombinasi Linier

PBB(a,b) dapat dinyatakan sebagai kombinasi linier (linear combination) a dan b dengan koefisien-koefisennya.

Contoh :

PBB(80, 12) = 4 ,
$4 = (-1) \cdot 80 + 7 \cdot 12.$

Dari sini dapat disimpulkan, misalkan a dan b bilangan bulat positif, maka terdapat bilangan bulat m dan n sedemikian sehingga PBB(a, b) = ma + nb

❖ Aritmetika Modulo

Misalkan terdapat dua buah bilangan bulat a dan m, dengan m > 0. Operasi a mod m (dibaca "a modulo m") memberikan sisa jika a dibagi dengan m. Pernyataan diatas dapat dinotasikan sebagai

$$a \bmod m = r$$

sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$.

m pada notasi disebut modulus atau modulo, dan hasil aritmetika modulo m terletak di dalam himpunan {0, 1, 2, …, m – 1}

❖ Kongruen

Kongruen dapat didefinisikan dengan misalkan a dan b bilangan bulat dan m adalah bilangan yang lebih besar dari 0, maka $a \equiv b \pmod m$ jika dan hanya jika m | (a – b).

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

❖ Balikan Modulo (modulo invers)

Di dalam aritmetika bilangan riil, balikan sebuah bilangan yang tidaknol adalah bentuk pecahannya sedemikian sehingga hasil perkalian keduanya sama dengan 1. Jika a adalah sebuah bilangan tidak-nol, maka balikannya adalah 1/a sedemikian sehingga a x 1/a = 1.

Contoh: Balikan 4 adalah 1/4, sebab 4 x 1/4 = 1.

Balikan a dilambangkan dengan a^{-1}. Di dalam aritmetika modulo, balikan modulo sebuah bilangan bulat lebih sukar dihitung

Balikan modulo hanya bisa dicari jika persamaannya memenuhi syarat, yaitu untuk sebuah bilangan bulat a(mod m) , jika a dan m relatif prima dan m > 1, maka balikan (invers) dari a (mod m) ada. Balikan dari a (mod m) adalah bilangan bulat x sedemikian sehingga: $xa \equiv 1 \pmod m$

Balikan modul dapat dinotasikan dengan

$$a^{-1} \pmod m = x$$

Pembuktiannya :

Terdapat dua buah bilangan bulat, a dan m, yang relatif prima, jadi PBB(a, m) = 1, dan terdapat bilangan bulat x dan y sedemikian sehingga:

$$xa + ym = 1$$

yang mengimplikasikan bahwa

$$xa + ym \equiv 1 \pmod m$$

Karena $ym \equiv 0 \pmod m$, maka

$$xa \equiv 1 \pmod m$$

Kekongruenan yang terakhir ini berarti bahwa x adalah balikan dari a (mod m).

❖ Kekongruenan Linier

Kekongruenan linier (linear congruence) berbentuk:

$$ax \equiv b \pmod m$$

Dimana m > 0, a dan b sembarang bilangan bulat, dan x adalah peubah bilangan bulat.

Pemecahan:

$ax = b + km \rightarrow$

$$x = \frac{b + km}{a}$$

❖ Sistem Kekongruenan Linier

Sistem kekongruenan linier terdiri dari lebih dari satu kekongruenan, yaitu:

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
...
$x \equiv a_n \pmod{m_n}$

Contoh:

Sebuah bilangan bulat jika dibagi dengan 3 bersisa 2 dan jika ia dibagi dengan 5 bersisa 3. Berapakah bilangan bulat tersebut?

Penyelesaian :

Misal bilangan bulat = x

x mod 3 = 2 → x 2 (mod 3)
x mod 5 = 3 → x 3 (mod 5)

Jadi, terdapat sistem kekongruenan:

$x \equiv 2 \pmod{3}$ (i)
$x \equiv 3 \pmod{5}$ (ii)

Untuk kekongruenan pertama:

$x = 2 + 3k_1$ (iii)

Substitusikan (iii) ke dalam (ii):

$2 + 3k_1 \equiv 3 \pmod{5} \rightarrow 3k_1 \equiv 1 \pmod{5}$

diperoleh

$k_1 \equiv 2 \pmod{5}$ atau $k_1 = 2 + 5k_2$

Substitusikan $k_1 = 2 + 5k_2$ ke dalam persamaan (iii):

$x = 2 + 3k_1$
$= 2 + 3 (2 + 5k_2)$
$= 2 + 6 + 15k_2$
$= 8 + 15k_2$
atau

$X \equiv 8 \pmod{15}$ (periksa bahwa 8 mod 3 = 2 dan 8 mod 5 = 3)

Semua nilai x yang kongruen dengan 8 (mod 15) juga adalah solusinya, yaitu x = 8, x = 23, x = 38, …, x = -7, dst

❖ Bilangan Prima

Bilangan bulat positif p (p > 1) disebut bilangan prima jika pembaginya hanya 1 dan p. Contoh dari bilangan prima adalah 23 karena ia hanya habis dibagi oleh 1 dan 23. Bilangan prima harus lebih besar dari 1, maka barisan bilangan prima dimulai dari 2, yaitu 2, 3, 5, 7, 11, 13, …. . Seluruh bilangan prima adalah bilangan ganjil, kecuali 2 yang merupakan bilangan genap.

Bilangan selain prima disebut bilangan komposit (composite). Misalnya 20 adalah bilangan komposit karena 20 dapat dibagi oleh 2, 4, 5, dan 10, selain 1 dan 20 sendiri. (The Fundamental Theorem of Arithmetic). Setiap bilangan bulat positif yang lebih besar atau sama dengan 2 dapat dinyatakan sebagai perkalian satu atau lebih bilangan prima

❖ Teorema Fermat

Pada Teorema Fermat dijelaskan, jika p adalah bilangan prima dan a adalah bilangan bulat yang tidak habis dibagi dengan p, yaitu PBB(a, p) = 1, maka:

$a^{p-1} \equiv 1 \pmod{p}$

Menurut teorema Fermat di atas, jika p adalah bilangan prima, maka $a^{p-1} \equiv 1 \pmod{p}$. Tetapi, jika p bukan bilangan prima, maka $a^{p-1} \not\equiv 1 \pmod{p}$.

B. Kriptografi

Kriptografi berasal dari Bahasa Yunani yaitu kryptos yang artinya tersembunyi dangraphein yang artinya tulisan. Maka secara bahasa kriptografi dapat diartikan sebagai “secret writing”.

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan dengan cara menyandikannya menjadi bentuk lain yang tidak bermakna. Tujuan dari penerapan ilmu kriptografi ini sendiri adalah agar pesan yang bersifat rahasia tidak dapat dibaca oleh pihakyang tidak berhak.

Kriptografi berkembang sedemikan rupa sehingga tidak lagi sebatas mengenkripsi pesan, tetapi juga memberikan aspek keamanan yang lain.

Menurut definisi baru, Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (message) [Schneier, 1996]. “art and science to keep message secure”.

Menurut definisi pembanding (Menez, 1996), Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi

Di dalam kriptografi terdapat istilah Pesan dan Cipherteks. Pesan disini adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Pesan ini dapat disebut juga sebagai plainteks (plaintext). Pesan yang dikirimkan ini dapat berbentuk berbagaiu rupa, antara lain teks, gambar, musik, mp3, video, tabel, daftar belanja, dan sebagainya. Selain itu, pesan juga dapat dibedakan menjadi pesan yang dikirim, comtohnya via pos, kurir, saluran telekom, dan ada pesan yang disimpan di dalam storage, contohnya dalam disk, kaset, dan CD. Kemudian Cipherteks, Cipherteks (ciphertext) adalah pesan yang telah disandikan sehingga tidak memiliki makna lagi. Tujuan dari Cipherteks ini adalah agar pesan tidak dapat dibaca oleh pihak yang tidak berhak. Nama lain dari Cipherteks adalah kriptogram (cryptogram).

Kemudian, ada yang nama Pengirim (sender), yaitu pihak yang mengirim pesan, dan ada yang namanya Penerima (receiver), yaitu pihak yang menerima pesan. Pengirim/penerima tidak hanya beropa orang tetapi juga bisa berupa komputer, mesin, dll.

Contoh Plainteks dan Cipherteks :

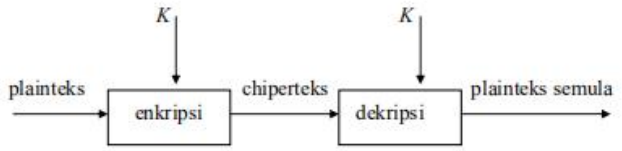
Plainteks: culik anak itu jam 11 siang

Cipherteks: t^$gfUi9rewoFpfdWqL:[uTcxZy

Selain itu, pada kriptografi juga dikenal istilah Enkripsi dan Dekripsi. Enkripsi (encryption) adalah proses menyandikan plainteks menjadi cipherteks. Sedangkan Dekripsi (decryption) adalah proses mengembalikan cipherteks menjadi plainteksnya.

Aplikasi dari proses Enkripsi-Dekripsi ini sangat banyak dalam kehidupan sehari-hari. Apalagi di zaman yang sangat canggih dan modern, ilmu ini sangat banyak digunakan. Contohnya dalam Pengiriman data melalui saluran komunikasi (data encryption on motion) dan Penyimpanan dokumen di

dalam disk storage (data encryption at rest).



Gambar 2.1 Proses Enkripsi dan Dekripsi secara Umum, diambil dari[5]

Proses enkripsi dan dekripsi ini dapat juga ditulis secara matematis. Misalkan:

C = chiperteks

P = plainteks

Fungsi enkripsi E memetakan P ke C,

E(P) = C

Fungsi dekripsi D memetakan C ke P,

D(C) = P

Fungsi enkripsi dan dekripsi harus memenuhi sifat:

D(E(P)) = P

❖ Algoritma kriptografi

Didalam Kriptografi, ada yang namanya Algoritma kriptografi yaitu langkah-langkah matematis yang digunakan untuk menyandikan pesan sehingga tidak diketahui lagi maknanya. Algoritma kriptografi itu sendiri dapat dibagi menjadi 3 macam :

1. Algoritma Simetris

Algoritma Simetris adalah algoritma yang dalam proses enkripsi dan proses dekripsi menggunakan kunci yang sama. Kunci yang dipakai saat enkripsi lah yang dipakai lagi saat dekripsi pesan. Contoh dari algoritma Simetris adalah RC.2, RC.4, RC.5, RC.6, Twofish, Advance Encryption Standart (AES), International Data Encryption Algorithm (IDEA), Data Encryption Standart (DES), On Time Pad (OTP), dan lain sebagainya.

2. Algoritma Asimetris

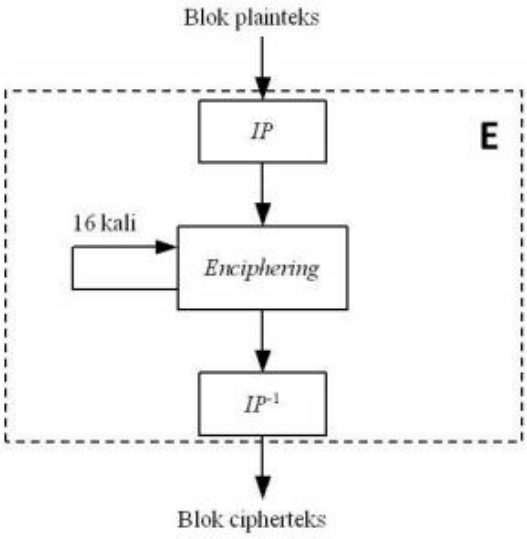
Algoritma Asimetris adalah algoritma yang dalam proses enkripsi dan proses dekripsi menggunakan kunci yang berbeda. Contoh kriptografi kunci publik diantaranya ElGamal, DSA (Digital Signature Algorithm), LUC, RSA(Rivest-Shamir-Adleman), Diffie-Hellman, dan lain sebagainya.

3. Fungsi Hash

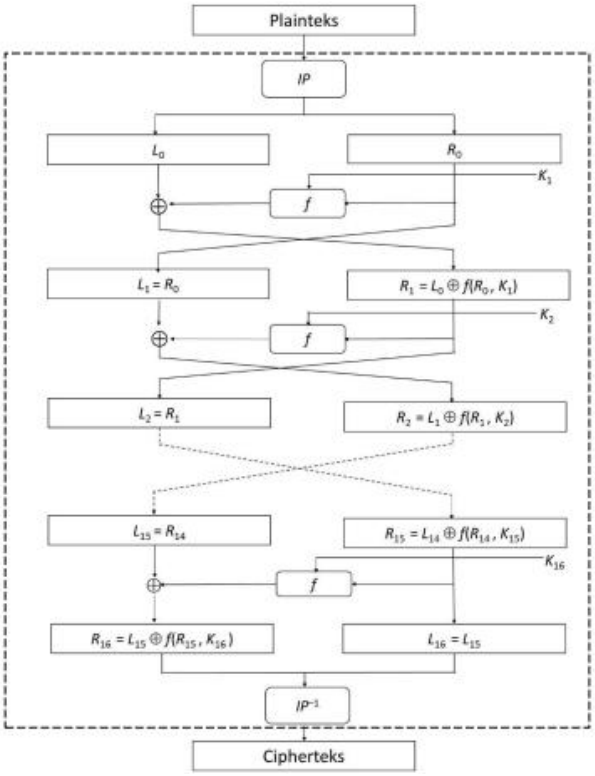
Suatu fungsi matematika yang mengambil input panjang variabel dan mengubahnya ke dalam bentuk biner dengan panjang yang tetap. Contoh fungsi hash adalah MD5 (Massage Digest 5), dan, SHA-1, SHA-2, SHA-3, MAC (Message Authentication Code) dan lain sebagainya.

❖ Data Encryption Standard (DES)

DES sendiri adalah standard, sedangkan algoritmanya yang digunakan pada DES adalah DEA (Data EncryptionAlgorithm). DES beroperasi pada ukuran blok 64 bit. Yang mana panjang kunci eksternalnya adalah 64 bit (sesuai ukuran blok), tetapi hanya 56 bit yang dipakai (8 bit paritas tidak digunakan). Setiap blok plainteks dienkripsi dalam 16 putaran enciphering. Setiap putaran menggunakan kunci internal berbeda. Kunci internal (48-bit) dibangkitkan dari kunci eksternal. Setiap blok mengalami permutasi awal (IP), 16 putaran enciphering, dan inversi permutasi awal (IP-1).



Gambar 2.2 Skema Global Algoritma DES, diambil dari [2]



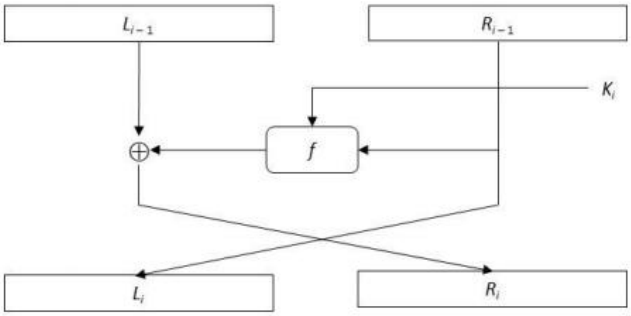
Gambar 2.3 Algoritma Enkripsi dengan DES, diambil dari [2]

a. Enciphering

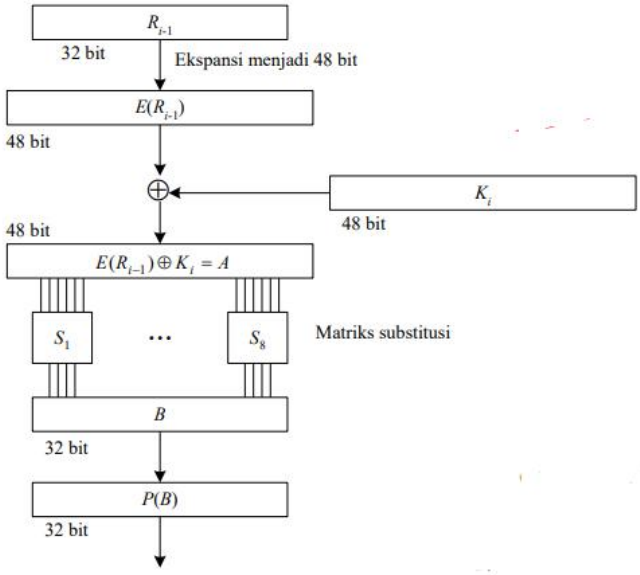
Setiap blok plainteks mengalami 16 kali putaran enciphering. Setiap putaran enciphering tersebut merupakan jaringan Feistel:

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$



Gambar 2.4 Satu putaran enciphering, , diambil dari [2]



Gambar 2.5 Diagram komputasi fungsi f:, diambil dari [2]

E adalah fungsi ekspansi yang memperluas blok R_{i-1} 32-bit menjadi blok 48 bit. Fungsi ekspansi direalisasikan dengan matriks permutasi ekspansi:

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Tabel 2.1, diambil dari [2]

Hasil ekpansi, yaitu $E(R_{i-1})$ di-XOR-kan dengan Ki menghasilkan blok A 48-bit:

$$E(R_{i-1}) \oplus K_i = A$$

Blok A dikelompokkan menjadi 8 kelompok, masing-masing 6 bit, dan menjadi masukan bagi proses substitusi. Ada 8 matriks substitusi, masing-masing dinyatakan dengan kotak-S. Kotak –S menerima masukan 6 bit dan memebrikan keluaran 4 bit.

Luaran proses substitusi adalah blok B yang panjangnya 32 bit. Blok B menjadi masukan untuk proses permutasi. Tujuan permutasi adalah untuk mengacak hasil proses substitusi kotak-S. Permutasi dilakukan dengan menggunakan matriks permutasi P (P-box) sbb:

16	7	20	21	29	12	28	17	1	15	23	26	5	8	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Tabel 2.2, diambil dari [2]

P(B) merupakan luaran dari fungsi f. Bit-bit P(B) di-XOR-kan dengan L_{i-1} menghasilkan R_i :

$$R_i = L_{i-1} \oplus P(B)$$

Jadi, luaran dari putaran ke-i adalah

$$(L_i, R_i) = (R_{i-1}, L_{i-1} \oplus P(B))$$

b. Dekripsi

Dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Pada proses dekripsi urutan kunci yang digunakan adalah K_{16}, K_{15}, …, K_1. Untuk tiap putaran 16, 15, …, 1, luaran pada setiap putaran deciphering adalah

$$R_{i-1} = L_i$$

$$L_{i-1} = R_i \oplus f(R_{i-1}, K_i) = R_i \oplus f(Li, Ki)$$

C. Automated Teller Machine (ATM)

Gambar 2.6 ATM (sumber : www.suluttoday.com)

Automated Teller Machine (ATM) atau dalam bahasa Indonesia Anjungan tunai mandiri adalah sebuah alat elektronik yang melayani nasabah bank untuk mengambil uang dan mengecek rekening tabungan mereka tanpa perlu dilayani oleh seorang "teller" manusia. Banyak ATM juga melayani penyimpanan uang atau cek, transfer uang atau bahkan membeli pulsa telepon seluler.

Mesin ATM pertama kali muncul pada itahun 1950-an di Amerika, Eropa, dan Jepang. Pada awalnya mesin ATM adalah mesin yang digunakan untuk meminjam uang kepada bank, di luar jam operasi bank atau ketika tidak sempat pergi ke bank. Namun, seiring dengan berkembangnya zaman, fungsi ATM pun semakin bertambah. Adapun beberapa fungsi ATM yang dapat digunakan pada saat sekarang ini adalah sebagai berikut.

1. Sarana Penarikan Uang Tunai

Ini merupakan fungsi utama ATM pada saat sekarang ini. ATM memudahkan nasabah dalam melakukan penarikan uang tunai. Selain keberadaannya yang ada dibanyak tempat, ATM

juga beroperasi selama 24 jam nonstop. Dibandingan dengan melakukan penarikan tunai ke bank yang memiliki jam operasi tertentu dan proses yang cukup panjang, melakukan penarikan tunai di ATM sangatlah mudah dan efisien.

2. Sarana Pengiriman Uang

Dengan adanya mesin ATM ini mempermudah nasabah dalam melakukan pengirimin uang ke rekening nasabah lainnya.

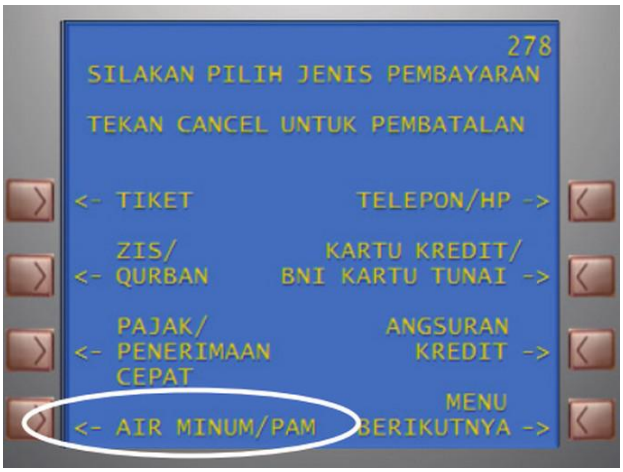
3. Sarana Penyetor Uang ke Rekening Tabungan

Selain untuk menarik uang tunai dan transfer, ATM juga dapat kita digunakan untuk menyetorkan uang tunai ke rekening kita sendiri atau mengirimkannya ke rekening orang lain.

Akan tetapi, tidak semua ATM dapat melakukan hal tersebut, biasanya ATM jenis ini ada di mall-mall atau pusat perbelanjaan. ATM ini pastinya memudahkan nasabah untuk menyetorkan uang tanpa harus berurusan dengan teller bank.

4. Membayar Tagihan dan Kebutuhan Lainnya

Selain itu, ATM juga dapat digunakan untuk membayar berbagai jenis tagihan dan membayar kebutuhan lainnya. Hal ini sangat memudahkan nasabah, karena dulu pembayar tagian seperti listrik dan air itu harus dilakuakn melalui loket pembayar resmi. Namun sekarang dapat melakukan pembayar tersebut melalui ATM yang ada dimana saja. Pembayaran lain yang dapat dilakuakan misalnya telepon, internet, TV kabel, asuransi hingga bayaran bidang pendidikan, sesuai dengan layanan atau bidang yang kita gunakan di ATM.



Gambar 2.7 Menu Pembayaran Tagihan pada ATM (sumber : www.saturadar.com)

III. PEMBAHASAN

Anjungan Tunai Mandiri atau Automatic Teller Machine (ATM) adalah suatu alat yang digunakan nasabah bank untuk melakukan transaski perbankan. Kegunaan utama dari ATM ini sendiri adalah untuk menarik uang secara tunai (cash withdrawal), namun saat ini ATM juga digunakan dapat untuk transfer uang (pemindahbukuan), mengecek saldo, membayar tagihan kartu ponsel, membeli tiket kereta api, dan sebagainya.

Dalam melakukan transaksi lewat ATM, kita memerlukan kartu magnetik (disebut juga kartu ATM) yang terbuat dari plastik dan kode PIN (Personal Information Number) yang berasosiasi dengan kartu tersebut. PIN ini sendiri terdiri dari 4 angka yang harus dijaga kerahasiannya oleh pemilik kartu ATM, sebab orang lain yang mengetahui PIN dapat menggunakan kartu ATM yang dicuri atau hilang untuk melakukan penarikan uang.

Kegunaan PIN ini adalah untuk memverifikasi kartu yang dimasukkan oleh nasabah di ATM. Proses verifikasi dilakukan di komputer pusat (host) bank, oleh karena itu harus ada komunikasi dua arah antara ATM dan komputer host. ATM mengirim PIN dan informasi tambahan pada kartu ke komputer host, host melakukan verifikasi dengan cara membandingkan PIN yang di-entry-kan oleh nasabah dengan PIN yang disimpan di dalam basisdata komputer host, lalu mengirimkan pesan tanggapan ke ATM yang menyatakan apakah transaksi dapat dilanjutkan atau ditolak.

Selama transmisi dari ATM ke komputer host, PIN harus dilindungi dari penyadapan oleh orang yang tidak berhak. Bentuk perlindungan yang dilakukan selama transmisi adalah dengan mengenkripsikan PIN. Di sisi bank, PIN yang disimpan di dalam basisdata juga dienkripsi.

Gambar 2.8 Mekanisme enkripsi dan dekripsi PIN pada transaksi dengan mesin ATM, diambil dari [8]

Algoritma enkripsi yang digunakan adalah DES dengan mode ECB. Karena DES bekerja dengan mengenkripsikan blok 64-bit, maka PIN yang hanya terdiri dari 4 angka (32 bit) harus ditambah dengan padding bits sehingga panjangnya menjadi 64 bit. Padding bits yang ditambahkan berbeda-beda untuk setiap PIN, bergantung pada informasi tambahan pada setiap kartu ATM-nya.

Karena panjang PIN hanya 4 angka, maka peluang ditebak sangat besar. Seseorang yang memperoleh kartu ATM curian atau hilang dapat mencoba semua kemungkinan kode PIN yang mungkin, sebab hanya ada $10 \times 10 \times 10 \times 10 = 10.000$ kemungkinan kode PIN 6-angka. Untuk mengatasi masalah ini, maka kebanyakan ATM hanya membolehkan peng-entry-an PIN maksimum 3 kali, jika 3 kali tetap salah maka ATM akan 'menelan' kartu ATM. Masalah ini juga menunjukkan bahwa kriptografi tidak selalu dapat menyelesaikan masalah keamanan data.

Beberapa jaringan ATM sekarang menggunakan kartu cerdas sehingga memungkinkan penggunaan kriptografi kunci publik. Kartu ATM pengguna mengandung kunci privat dan sertifikat digital yang ditandatangani oleh card issuer (CA) untuk mensertifikasi kunci publiknya. ATM mengotentikasi kartu dengan cara mengirimkan suatu string ke kartu untuk ditandatangani dengan menggunakan kunci privat, lalu tanda-

tangan tersebut diverifikasi oleh ATM dengan menggunakan kunci publik pemilik kartu. Seperti semua sistem yang berbasis sertifikat digital, terminal ATM perlu memiliki salinan kunci publikcard issuer dengan maksud untuk memvalidasi sertifikat digital. Hal ini direalisasikan dengan menginstalasi kunci publik tersebut ke dalam mesin ATM.

Adapun proses dalam pengamanan PIN dalam sistem keamanan ATM, sebagai berikut.

1. Pertama, sistem akan mengambil 5 digit terakhir dari nomor rekening kita .
2. Kemudian, sistem akan menggabungkan kelima angka tadi dengan 11 digit dari data valisasi yang diciptakan sendiri oleh sistem.
3. Maka akan diperoleh 16 angka yang ukurannya 16 bit, ini akan menjadi kunci PIN untuk dimasukkan dalam algoritma DES.
4. Setelah diproses menggunakan algoritma DES, akan diambil 4 digit pertama dari hasil pemrosesannya, yang kemudian diubah ke bentuk decimal. Setelah itu akan diubah lagi ke dalam bentuk heksadesimal oleh DES. Yang kemudian 4 digit tersebut disebut "PIN alami".
5. Setelah PIN alami tersebut didapatkan akan ditambah dengan 4 digit baru yang disebut offset dan kemudian mengahasilkan PIN yang siap digunakan oleh nasabah.

IV. STUDI KASUS

Misalkan seorang Nasabah ingin melakukan transaksi penarikan uang tunai di ATM. Nasabah ini memiliki rekening yang nomornya 4506602100091715. Sesampainya di ATM, ia memasukkan kartu ATM-nya ke dalam mesin ATM. Kemudian mesin ATM, akan memvalidasi kita sebagai pemilik kartu ini. Adapun langkahnya sesuai dengan penjelasan pada BAB sebelumnya, yaitu sebagai berikut.

1. Dari nomor rekening yang dimiliki nasabah, diambil 5 digit terakhit, yaitu 91715
2. Kemudian lima digit tadi digabungkan dengan 11 digit data validasi 88070123456. Maka akan diperoleh 16 digit angka, yaitu 8807012345691715
3. Pada mesin ATM telah tersedia "Kunci PIN" dari Algoritma DES, yaitu FEFEFEFEFEFEFEFE yang juga terdiri dari 16 digit angka. Kemudian akan diproses dengan mengubah bentuknya oleh metode DES sampai nilainya menjadi A2CE126C69AEC82D. dari nilai tersebut diambil 4 digit pertama yang akan diproses lagi oleh algoritma DES untuk mendapatkan "PIN Alami", yang mana akan didapatkan PIN alaminya 0224
4. "PIN Alami" yang telah iddapatkan tadi ditambahkan dengan offset-nya 6565.
5. Hasilnya menjadi 0224 + 6565 = 6789 yang mana 4 digit ini merupakan nomor PIN nasabah.

Nomor inilah yang akan disimpan ke dalam pita magnetik yang ada pada kartu ATM yang dimiliki nasabah. Nomor ini disimpan bersama dengan data penting lainnya, seperti nomor rekening, nomor kartu, dan sebagainya.

V. KESIMPULAN

Teori bilangan adalah cabang matematika murni yang ditujukan untuk mempelajari bilangan bulat (integer) atau fungsi bernilai bilangan bulat. Konsep teori bilangan ini dapat diaplikasikan dibanyak hal, salah satu pada bidang kriptografi. Penerapan teori bilangan pada kriptografi ini memiliki peran yang sangat penting dalam menjamin keamanan ketika melakukan transaksi menggunakan mesin ATM. Penerapan dari konsep kriptografi ini adalah pada proses enkripsi PIN yang dimasukan nasabah ketika sedang melakukan transmisi data dati ATM ke bank untuk dilakukan proses validasi. Kemudian juga berperan dalam menenkripsi data nasabah yang disimpan di bank. Hal ini agar data tersebut tidak dapat disadab oleh orang yang tidak bertanggungjawab. Proses enkripsi PIN nasabah ini menggunakan algoritma DES yang ada pada algoritma kriptografi. Yang mana setelah proses enkripsi ini, PIN nasabah menjadi tidak bisa dikenali oleh pihak lain.

VI. PENUTUP

Segala puji bagi Allah SWT yang telah memberikan penulis kemudahan sehingga dapat menyelesaikan makalah ini dengan tepat waktu. Penulis mengucapkan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, M.T selaku dosen mata kuliah Matematika Diskrit kelas K01 yang telah memberi materi untuk penulisan makalah. Tidak lupa juga penulis mengucapkan terima kasih kepada kedua orang tua serta teman-teman yang telah memberi dukungan selama pengerjaan makalah ini. Akhir kata, penulis menyadari masih terdapat kekurangan dan kesalahan kata dalam makalah ini, penulis berharap makalah ini dapat digunakan sebaik-baiknya dan dikembangkan sehingga lebih menghasilkan manfaat bagi masyarakat luas

REFERENSI

[1] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". Introduction to Modern Cryptography.
[2] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Review-beberapa-block-cipher-dan-stream-cipher-2020-bagian1.pdf diakses pada 8 Desember 2020 pukul 20.00
[3] http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian1.pdf diakses pada 6 Desember 2020 pukul 19.00
[4] http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian2.pdf diakses pada 6 Desember 2020 pukul 19.05
[5] http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian3.pdf diakses pada 6 Desember 2020 pukul 19.10
[6] https://www.saturadar.com/2019/09/Pengertian-ATM.html pada 8 Desember 2020 pukul 21.00
[7] Merriam-Webster Dictionary. Springfield, MA: Merriam-Webster.
[8] https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Kriptografi%20dalam%20Kehidupan%20Sehari-hari%20(Bagian%201).pdf pada 8 Desember 2020 pukul 20.30

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.

Padang, 11 Desember 2020

Nabila Hannania 13519097