Penerapan Teori Bilangan Bulat dan Bilangan Prima dalam Pencegahan Penyadapan Informasi di Dunia Maya

Steve Immanuel Harnadi / 13512035
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13512035@std.stei.itb.ac.id, steve.harnadi@gmail.com

***Abstract*—Bilangan bulat dan bilangan prima merupakan suatu fenomena yang tidak asing lagi dalam kehidupan sehari-hari. Teori bilangan itu sendiri memiliki proses sejarah yang sangat panjang mulai dari bangsa Babilonia, Mesir kuno, India, hingga pada era masehi dengan tokoh-tokoh terkenal seperti Pierre de Fermat (1601-1665), Jamshid Al-Kashi (1380 M), Abu Ali Hasan Ibnu Al-Haytam (965 M), dan lain-lain.**

Baik teori bilangan bulat maupun bilangan prima itu sendiri erat kaitannya dengan operasi sisa bagi yang disebut dengan modulo. Aplikasi operasi ini salah satunya digunakan dalam proses penyandian data (dalam hal ini untuk menangani proses penyadapan informasi-informasi penting) yang disebut kriptografi.

Makalah ini berisi pendahuluan, dasar teori bilangan bulat, bilangan prima, dan kriptografi, metode-metode penyandian informasi, analisis kelebihan dan kekurangan metode, dan kesimpulan.

***Kata Kunci*—Bilangan bulat dan prima, kriptografi, metode penyandian, penyadapan.**

I. PENDAHULUAN

Pada masa dewasa ini, kita masih diperhadapkan dengan banyaknya kasus-kasus kriminal yang semakin lama semakin kompleks. Modus yang dipakai pelaku kriminal pun bermacam-macam, bukan hanya melalui ancaman atau intimidasi secara fisik, melainkan juga bisa terselubung di dunia maya. Modus yang terakhir ini mungkin kelihatan langka namun tidak bisa dianggap remeh karena banyak sekali informasi-informasi penting yang bisa dimanfaatkan oleh pelaku kriminal untuk melaksanakan aksi kriminalnya.

Salah satu kejahatan dunia maya yang akan dibahas lebih jauh dalam makalah ini adalah tindakan penyadapan yang dilakukan oleh salah satu pihak untuk mendapatkan informasi-informasi penting dan rahasia. Contohnya adalah penyadapan yang dilakukan oleh salah satu badan intelijen Australia terhadap kegiatan-kegiatan politik yang dilakukan di Indonesia baru-baru ini. Meskipun bukan merupakan tindakan kriminal, namun hal tersebut berakibat memburuknya hubungan kedua negara tersebut. Jika informasi yang disadap tersebut sudah berkaitan dengan dokumen negara yang penting, maka kasus tersebut bisa saja berujung pada peperangan politis kedua negara yang pada akhirnya harus diselesaikan di bawah naungan PBB.

Contoh lain yang tidak jauh berbeda dengan kasus sebelumnya adalah kejahatan di *facebook*. Bentuk yang digunakan oleh pelaku bisa bermacam-macam, misalnya mengambil alih akun *facebook* orang lain, menggunakan identitas palsu untuk menjerat korban demi kepentingan tertentu, dan penggunaan aplikasi palsu untuk menipu pelanggan yang menggunakannya. Jadi, kejahatan di *facebook* pun merupakan kejahatan dunia maya yang erat kaitannya dengan keamanan informasi. Jika kita tidak siap menanggulanginya, maka kejahatan jenis ini akan semakin menjadi di era informasi ini.

Kasus-kasus yang disebutkan sebelumnya hanyalah sebagian kecil dari banyaknya kasus kejahatan dunia maya di mana pencurian informasi menjadi kunci utamanya. Karena itu, informasi penting sekecil apa pun perlu disandikan dengan metode-metode/algoritma-algoritma tertentu, yang akan dibahas pada bab-bab selanjutnya. Untuk memahami proses penyandian tersebut, maka teori bilangan bulat dan bilangan prima menjadi penting untuk dipahami karena menjadi landasan teori yang paling utama dari kriptografi (proses penyandian) itu sendiri.

. II. DASAR TEORI

Bilangan bulat merupakan suatu elemen yang bersifat diskrit (terpisah). Artinya, bilangan bulat berbeda dengan bilangan pecahan atau desimal yang bersifat kontinu karena bilangan 3,001 dan 3,00001 adalah kedua bilangan desimal sehingga tidak bisa dipastikan batas-batas cakupan bilangan desimal tersebut. Dengan kata lain, bilangan bulat adalah bilangan yang tidak mempunyai unsur pecahan desimal. Contoh bilangan bulat : ....-3,-2,-1,0,1,2,3,.....

Dalam pembahasan kali ini, sifat bilangan bulat yang hendak diperdalam adalah sifat pembagian bilangan bulat. Sifat ini diperdalam melalui suatu ilmu yang disebut aritmetika. Salah satu tokoh yang terkenal memperdalam ilmu ini adalah Euclides yang melahirkan suatu algoritma yang berkaitan dengan sifat pembagian bilangan bulat yang kemudian disebut algoritma Euclidean.

Bilangan prima adalah kasus khusus dari bilangan bulat. Bilangan prima adalah bilangan bulat yang hanya

habis dibagi oleh bilangan 1 dan bilangan itu sendiri. Contoh bilangan prima : 2,3,5,7. Banyak teori yang mendukung bilangan prima yang akan dibahas lebih lanjut. Bilangan prima inilah yang kemudian diaplikasikan dalam proses kriptografi.

Teori dasar pembagian bilangan bulat dapat dijabarkan sebagai berikut :

> "Misalkan a dan b adalah dua buah bilangan bulat dengan syarat a ≠ 0. Maka a habis membagi b jika terdapat bilangan bulat c sedemikian sehingga b = ac" [Rinaldi Munir, 2006]

Notasi umum yang menyatakan teori di atas :

a | b jika b = ac, c € Z dan a ≠ 0.

Z = himpunan bilangan bulat

Dengan kata lain, hasil pembagian b dengan a haruslah bilangan bulat. Sering juga disebutkan bahwa a kelipatan b. Maknanya serupa hanya berbeda sudut pandang saja.

Teorema berikut merupakan teorema dasar pembagian bilangan bulat lain yang jauh lebih penting dari teori sebelumnya, karena mencakup juga sisa bagi dari pembagian sebuah bilangan bulat a oleh bilangan bulat b misalnya. Teorema ini disebut juga sebagai teorema Euclidean yang berbunyi :

> Misalkan m dan n adalah dua buah bilangan bulat dengan syarat n > 0. Jika m dibagi dengan n maka terdapat dua buah bilangan bulat unik q (quotient) dan r (remainder) sedemikian sehingga
>
> m = nq + r
>
> dengan 0 ≤ r ≤ n [Rinaldi Munir, 2006]

Dengan teorema tersebut, kita dapat menyimpulkan bahwa jika suatu bilangan bulat m dibagi dengan n pasti menghasilkan suatu konstata yang disebut hasil bagi dan sisa bagi (tidak boleh negatif).

Bilangan bulat mengandung faktor yang habis membagi bilangan itu sendiri. Misalnya bilangan 24 mempunyai faktor 1,2,3,4,6,8,12,24. Konsep faktor bilangan ini mendasari konsep FPB (faktor persekutuan terbesar). Jadi, misalkan ada bilangan bulat lain yaitu 20 memiliki faktor 1,2,4,5,10,20, maka FPB dari 20 dan 24 dapat dilihat dari faktor pembagi bersama antara kedua bilangan tersebut yang paling besar. Berarti, dapat disimpulkan FPB dari 20 dan 24 adalah 4 karena faktor pembagi bersama yang lain (1 dan 2) bukan merupakan pembagi terbesar kedua bilangan tersebut. Adapun definisi formal dari FPB :

> Misalkan a dan b adalah dua buah bilangan bulat tidak nol. Pembagi bersama terbesar (PBB) dari a dan b adalah bilangan bulat terbesar d sedemikian sehingga d | a dan d | b. Dalam kasus ini, kita menyatakan bahwa PBB (a,b) adalah d [Rinaldi Munir, 2006].
> Keterangan : PBB nama lain dari FPB.

Adapun algoritma yang paling efisien yang digunakan untuk mencari FPB antara kedua buah bilangan bulat disebut juga sebagai algoritma Euclidean (tidak dibahas karena kurang berkaitan dengan topik makalah ini).

FPB juga dapat dinyatakan dalam bentuk lain yaitu bentuk kombinasi lanjar. Kombinasi lanjar di sini maksudnya dalam bentuk persamaan linear. Jadi, jika terdapat dua buah bilangan bulat a dan b positif, maka pasti terdapat bilangan bulat m dan n sedemikian sehingga : ma + nb = FPB (a,b). Perlu diketahui bahwa kedua bilangan yang relatif prima (nilai FPB kedua bilangan tersebut 1) mempunyai bentuk homogen lanjar : ma + nb = 1.

Teorema yang sudah dipaparkan di atas hanyalah langkah awal untuk lebih memahami inti dari teori bilangan itu sendiri, yaitu aritmetika modulo yang merupakan dasar dari aplikasi kriptografi. Aritmetika modulo merupakan pengembangan dari teori-teori yang sudah dijabarkan sebelumnya, karena berkaitan juga dengan sisa bagi antara dua buah bilangan bulat. Operator yang dipakai dalam aritmetika modulo ini adalah operator mod (sisa bagi). Misalkan : 6 mod 4 = 2, 12 mod 7 = 5, 13 mod 9 = 4. Definisi yang lebih formal terkait aritmetika modulo :

> Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi a mod m (dibaca "a modulo m") memberikan sisa jika a dibagi dengan m. Dengan kata lain, a mod m = r sedemikian sehingga a = mq+ r, dengan 0 ≤ r <m.[Rinaldi Munir, 2006]

Notasi operasional yang digunakan untuk menyatakan operasi aritmetika modulo : a mod m = r, dengan r adalah sisa bagi dari a dibagi dengan m.

Operasi mod berguna untuk menyatakan kekongruenan modulo , yaitu kekongruenan dua buah bilangan bulat dalam hal sisa bagi, dan ditulis dengan operasi "≡". Misalkan terdapat bentuk kekongruenan modulo 8 ≡ 4 (mod 2), artinya 8 mod 2 = 4 mod 2 = 0. Contoh lainnya 38 ≡ 13 (mod 5) karena 38 mod 5 = 13 mod 5 = 3. Jika kedua buah bilangan bulat tidak kongruen modulo, maka simbol keduanya dinyatakan dengan tanda "≡/". Misalkan, 41 ≡/ 30 (mod 3) karena 41 mod 3 = 2 sedangkan 30 mod 3 = 0. Teorema yang menyatakan kekongruenan modulo :

> Misalkan a dan b adalah bilangan bulat dan m adalah bilangan > 0, maka a ≡ b (mod m) jika m habis membagi a-b
> [Rinaldi Munir, 2006]

Bilangan prima secara teori mempunyai definisi sebagai bilangan yang lebih besar sama dengan 2 yang pembaginya hanya bilangan 1 dan bilangan itu sendiri. Bilangan selain bilangan prima disebut juga bilangan komposit. Secara umum, teori yang menyatakan karakteristik bilangan prima disebut juga teori fundamental aritmetik, yang menyatakan bahwa setiap bilangan positif yang lebih besar sama dengan 2 dapat dinyatakan sebagai hasil perkalian 1 atau lebih bilangan prima. Teori yang mendukung keabsahan bilangan prima dan sering digunakan adalah Teorema Fermat. Bunyi teorema tersebut dijabarkan sebagai berikut :

Jika p adalah bilangan prima dan a adalah bilangan bulat yang tidak habis dibagi dengan p, yaitu PBB (a,p) = 1, maka :

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

Sayangnya, masih terdapat kebocoran pembuktian keabsahan bilangan prima dengan teorema fermat. Misalkan bilangan komposit 341 (karena habis dibagi 11 dan 31 selain 1 dan 341, berarti bukan bilangan prima) yang memenuhi teorema fermat berikut :

$$2340 \equiv 1 \pmod{341}$$

sehingga bilangan 341 disebut juga bilangan prima semu (*pseudoprimes*). Hanya saja, karena jumlah bilangan semacam itu sedikit, teorema ini masih dapat ditoleransi.

Setelah membahas secara ringkas teori-teori dasar mengenai bilangan bulat, peneliti akan mulai membahas mengenai dasar-dasar dari kriptografi yang merupakan topik utama yang dikaji dalam makalah ini. Perlu Anda ketahui bahwa ilmu kriptografi saat ini sudah meluas dan hampir semua pakar IT menguasainya, terutama setelah tahun 1980 saat perang dingin berakhir.

Kriptografi sendiri secara asal-usul kata berasal dari bahasa Yunani, yaitu dari kata *kripto* yang berarti *secret* (rahasia) dan *graphia* yang berarti *writing* (tulisan). Secara harfiah, kriptografi artinya ilmu atau seni untuk menjaga keamanan pesan ketika suatu pesan dikirim dari satu tempat ke tempat lain. Unsur-unsur yang terkandung di dalam kriptografi adalah sebagai berikut :

1. Pesan adalah data dan informasi yang dapat dibaca dan dimengerti maknanya, disebut juga sebagai Plainteks.
2. Chiperteks adalah pesan yang sudah diterjemahkan menjadi kode/sandi yang tidak bisa dipahami atau dimengerti maknanya. Sedangkan istilah Chiper mengacu kepada algoritma yang menerjemahkan kode tersebut.
3. Dalam kriptografi, tentu saja terdapat unsur pengirim dan penerima yang memegang peranan vital dalam proses pengiriman pesan.
4. Proses pengubahan Plainteks menjadi Chiperteks disebut juga sebagai Enkripsi. Sedangkan, proses sebaliknya (mengubah Chiperteks menjadi Plainteks semula) disebut Deskripsi.
5. Penyadap yang bertujuan untuk mencuri informasi/pesan yang sedang dikirim.
6. Kriptografer adalah orang yang ahli dalam melakukan ekripsi maupun deskripsi.
7. Kriptanalis adalah orang yang menganalisa metode enkripsi dan chiperteks dengan tujuan menemukan kembali teks aslinya.

Metode kriptografi pada intinya menggunakan algoritma dalam proses pengerjaannya. Secara umum metode yang digunakan dalam kriptografi terbagi menjadi dua, yaitu metode penyandian klasik dan metode penyandian modern. Metode penyandian klasik masih menggunakan metode yang sederhana. Metode enkripsi yang tergolong sebagai kriptografi klasik diantaranya adalah metode penyadian transposisi, metode penyandian substitusi, dan metode penyandian Caesar pada masa Romawi kuno. Sedangkan metode enkripsi yang sudah tergolong mutakhir menggunakan algoritma-algoritma yang rumit seperti misalnya algoritma kunci simetris (contohnya algoritma DES) dan algoritma kunci nonsimetris (contohnya algoritma RSA,DSA, dan Diffie-Hellman). Namun, yang menjadi pokok bahasan dalam makalah ini adalah algoritma enkripsi yang memanfaatkan teori bilangan bulat, sehingga algoritma kunci nonsimetri dijadikan acuan dalam pembahasan makalah ini. Secara umum, menurut *Shannon*, algoritma yang dipakai dalam kriptografi harus memiliki kekuatan untuk melakukan konfusi dan difusi.

1. Konfusi (*confusion*) : memiliki kemampuan mengaburkan hubungan antara *plaintext* dan *chipertext*. Konfusi menimbulkan kesulitan dalam usaha musuh untuk mencari keteraturan pola antara *plaintext* dan *chipertext*. Contoh metode yang memanfaatkan sifat ini adalah metode substitusi (akan dibahas kemudian).
2. Difusi (*difusion*) : menyebarkan redundansi plaintext dengan menyebarkan masukan ke seluruh chipertext. Contoh metode yang memanfaatkan sifat ini adalah metode transposisi (akan dibahas kemudian).

Dalam aplikasi kriptografi yang dibahas dalam makalah ini, metode enkripsi yang digunakan lebih ditekankan kepada metode mutakhir dan modern sebab pada era dewasa ini algoritma-algoritma rumit lebih sering digunakan daripada algoritma yang konvensional.

Istilah Kriptografi sendiri tampaknya perlu dibedakan dengan istilah *Steganografi* yang hampir serupa. Steganografi merupakan suatu teknik untuk menyembunyikan pesan/ rahasia antara pengirim dan penerima sehingga tidak ada seorang pun yang menyadari adanya pesan rahasia. Sedangkan kriptografi bertujuan untuk menyamarkan arti dari pesan yang dikirim namun tidak menyembunyikan/menyelubungi pesan yang dikirim.

III. APLIKASI KRIPTOGRAFI DENGAN TEORI BILANGAN BULAT UNTUK MELINDUNGI INFORMASI PENTING DI DUNIA MAYA DARI PENYADAPAN

Sebelum membahas lebih lanjut bagaimana aplikasi sesungguhnya teori bilangan bulat dalam kriptografi, penulis hendak menguraikan dulu ruang lingkup informasi dunia maya yang dimaksud dalam makalah ini karena dunia maya memiliki cakupan yang luas, namun tidak semuanya dapat dibahas di makalah ini. Ada pun informasi dunia maya yang penting untuk dibahas :

1. Akun pribadi *facebook* dan cara perlindungannya dari serangan hacker. Contoh sandi yang hendak dienkripsikan :

   A345ZZZZZ@9529710

2. Nomor PIN ATM dan cara perlindungannya dari pelaku kriminal yang hendak membobol nomor tersebut. Contoh nomor PIN ATM yang hendak dienkripsikan :

   7640921456781236

Kedua informasi di atas sangat penting untuk dilindungi dengan ilmu kriptografi, sebab jika sudah bocor ke pihak-pihak yang tidak diinginkan, maka mungkin saja hal-hal yang membahayakan korban terjadi. Karena itu, pada pembahasan ini dipaparkan metode kriptografi mulai dari metode klasik sampai metode mutakhir.

3.1 Metode Kriptografi Klasik

Metode enkripsi klasik meliputi metode substitusi, transposisi, dan penyandian Caesar dengan teknik penyandiannya masing-masing. Algoritma yang digunakan dalam metode-metode tersebut pada umumnya masih merupakan algoritma sederhana dan belum banyak menggunakan aplikasi aritmetika modulo. Sistem penyandiannya pun hanya satu arah, artinya hanya kriptografer yang mengetahui kunci untuk memecahkan teks hasil enkripsi.

Ide dari metode enkripsi substitusi adalah menukar susunan huruf atau karakter pada sandi lewat atau nomor PIN dengan algoritma kunci tertentu yang menggantikan suatu karakter tertentu. Diketahui deret-deret huruf asli (plaintext) sebagai berikut :

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

Hasil enkripsi dengan menggunakan metode ini terdiri atas bermacam-macam hasil bergantung dari algoritma kunci yang digunakan :

1. Memakai Algoritma Deret Langsung

   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

2. Memakai Algoritma Deret Inversi

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

3. Memakai Algoritma Deret Acak Tidak Berkunci

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

4. Memakai Algoritma Deret Acak Berkunci

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

5. Memakai Algoritma Deret Acak Berkunci Inversi

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

Chiperteks hasil enkripsi dengan metode ini biasanya dikelompokkan dalam blok-blok yang terdiri dari empat atau lima karakter agar menghilangkan karakteristik teks aslinya. Selain itu, pengelompokan ini digunakan untuk menekan biaya pengeluaran saat itu.

Ide dari metode enkripsi transposisi bisa dikatakan sedikit lebih unik daripada metode enkripsi substitusi sebelumnya, yaitu mengubah letak karakter dari posisi semula. Akibatnya variasi metode enkripsi transposisi cukup banyak karena terdapat banyak cara mengubah letak huruf atau karakter pada sandi lewat atau nomor PIN ATM. Berikut adalah variasi pengubahan letak karakter dengan contohnya :

1. Transposisi *Rail Fence*
   Cara yang dilakukan adalah menuliskan teks asli dalam bentuk pagar imajiner naik turun, kemudian membaca teks asli secara horizontal per baris. Misalkan terdapat teks asli : SAYA PERGI, maka penulisan teks asli tersebut secara *rail fence* adalah :
   S----------P--------I----------Lajur1
   ---A--- A---E----G----------Lajur2
   -------Y--------R----------Lajur3
   Sehingga hasil enkripsi teks tersebut dibaca per lajur menjadi : SPI AAE GYR (penulisan teks enkripsi per blok tiga karakter).
2. Transposisi *Route*
   Cara yang dilakukan transposisi ini hampir sama dengan transposisi *Rail Fence*, yaitu menulis teks asli secara naik turun per kolom. Namun, algoritma pembacaan teks tersebut lebih kompleks daripada pembacaan teks hasil transposisi *Rail Fence*. Arah pembacaan teks metode ini biasanya spiral dimulai dari kanan atas ke kiri bawah dan sebagainya.
3. Transposisi Kolom
   Cara yang dilakukan transposisi ini adalah dengan cara menuliskan teks asli per baris dengan panjang kolom yang telah ditentukan sebagai kuncinya. Kemudian, dilakukan pembacaan per kolom dengan urutan per kolomnya diacak dari urutan semula. Misalkan terdapat teks asli : CEPAT PULANG MUSUH HENDAK MENYERANG KITA, maka penulisan teks tersebut (dengan kunci misalnya sasak (artinya ada 5 kolom)) :

1	2	3	4	5
C	E	P	A	T
P	U	L	A	N
G	M	U	S	U
H	H	E	N	D
A	K	M	E	N
Y	E	R	A	N
G	K	I	T	A

   Urutan kolom tersebut dibalik pembacaannya menjadi seperti berikut :

5	1	4	2	3
C	E	P	A	T
P	U	L	A	N
G	M	U	S	U
H	H	E	N	D
A	K	M	E	N
Y	E	R	A	N
G	K	I	T	A

   Sehingga pembacaan per kolom dari kolom 1-5 menghasilkan chiperteks : EUMHK EKAAS NEATT NUDNN APLUE MRICP GHAYG (pengelompokan per blok 5 karakter).

4. Transposisi Ganda
   Transposisi ini merupakan pengembangan dari transposisi kolom yang diperumit. Artinya, setelah dihasilkan chiperteks hasil transposisi kolom, maka chiperteks tersebut dienkripsikan lagi urutannya dengan transposisi kolom ganda sehingga transposisi ganda bisa disebut juga transposisi kolom ganda.
5. Transposisi Myszkowski
   Transposisi ini juga merupakan variasi dari transposisi kolom hanya penulisannya sekarang ditulis per baris. Transposisi ini ditemukan oleh Émile Victor Théodore Myszkowski di tahun 1902. Pembeda transposisi ini dibandingkan transposisi kolom adalah permutasi kata kunci yang dilakukan. Misalnya, pada transposisi kolom kata kunci yang dipakai adalah sasak (1 2 3 4 5), maka pada transposisi ini kata kunci sasak diterjemahkan menjadi 1 3 3 4 2 tergantung bentuk permutasinya.
   Misalkan terdapat pesan asli : CEPAT PULANG MUSUH HENDAK MENYERANG KITA, maka penulisan teksnya :

1	3	3	4	2
C	E	P	A	T
P	U	L	A	N
G	M	U	S	U
H	H	E	N	D
A	K	M	E	N
Y	E	R	A	N
G	K	I	T	A

   Pembacaan dari hasil penulisan teks di atas dilakukan per baris berdasarkan urutan nomor permutasinya, sehingga teks enkripsi yang dihasilkan : CPGHA YGTNU DNNAE PULMU HEKME RKIAA SNEAT (pengelompokan per blok 5 karakter).

Sedangkan ekripsi dengan metode Caesar sebenarnya merupakan pengembangan dari metode substitusi namun dengan kunci yang menggunakan konsep aritmetika modulo. Kelebihan metode enkripsi ini dari metode klasik sebelumnya adalah pada metode ini, penerima pesan dapat lebih mudah mendeskrisipkan kembali chiperteks ke teks asli semula jika dibandingkan dengan metode sebelumnya. Cara pembacaan plainteksnya adalah dengan memperhatikan urutan hurufnya di urutan alphabetik. Adapun kunci yang digunakan dalam metode Caesar dapat dituliskan dalam bentuk fungsi sebagai berikut :

> Enkripsi : C = E(P) = (P + k) mod 26
> Deskripsi : P = D(C) = (C – k) mod 26
> dengan P adalah plainteks, C adalah chiperteks, dan k adalah jumlah pergeseran karakter yang diinginkan (yang juga merupakan kunci yang harus dijaga kerahasiannya).

Jadi, misalkan kita menginginkan pergeseran karakter dari karakter semula sebanyak 4 karakter, maka jika huruf asli adalah ‘a’ yang berarti urutan 1, maka hasil enkripsi terhadap huruf ‘a’ adalah huruf dengan urutan (1 + 4) mod 26 = 5 yang berarti adalah huruf ‘e’. Proses deskripsinya berarti kebalikan dari proses enkripsi. Misalkan terdapat deret huruf sandi : AEJMNAB. Maka chiperteks dari deret huruf tersebut dengan kunci pergeseran 3 adalah DHMPQDE.

3.2 Metode Kriptografi Mutakhir

Metode kriptografi ini sudah menggunakan algoritma-algoritma yang lebih rumit dan sistem kerjanya bersifat dua arah, artinya baik pengirim maupun penerima pesan sama-sama mengetahui kunci yang digunakan dalam deskripsi dan enkripsi pesan sehingga kerahasiaan data yang dikirim bisa lebih terjamin. Karena sistem kerjanya yang dua arah, maka kunci yang digunakan pada metode ini juga ada dua, yaitu kunci publik (kunci enkripsi, yang boleh diketahui publik) dan kunci privat (kunci deskripsi, yang harus dirahasiakan).

Sesuai dengan lingkup pembahasan dalam makalah ini, yaitu melindungi akun facebook dan nomor PIN ATM dari serangan pihak luar yang tidak bertanggung jawab, maka metode enkripsi dengan algoritma DSA, RSA, maupun Diffle-Hellman ini menjadi lebih mendesak untuk digunakan dari segi keamanan teks hasil enkripsi. Di samping algoritmanya yang kompleks, kunci yang dipakai pun bersifat dua arah sehingga menyulitkan hacker maupun pelaku kriminal membobol sandi-sandi rahasia yang dimiliki pemilik akun atau nomor ATM.

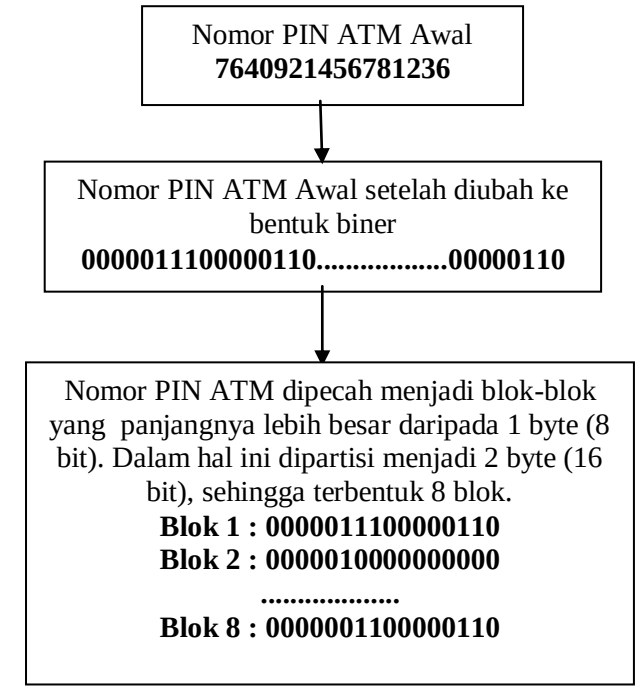
Penulis mengambil contoh akun facebook dan nomor PIN ATM seperti yang tertulis dalam makalah ini (halaman 4 kolom kiri). Baik akun facebook maupun nomor PIN ATM tersebut sebenarnya bisa dienkripsikan dengan metode klasik seperti yang sudah dipaparkan sebelumnya, namun perlu diketahui juga bahwa proses deskripsi data dari sudut pandang pemakai akun atau nomor tidaklah mudah. Di samping itu, penulis merasa masih terdapat kebocoran pola jika memakai algoritma klasik seperti yang dipaparkan sebelumnya. Karena itu, penyandian informasi penting lebih kuat jika memakai algoritma yang memanfaatkan teori bilangan bulat (khususnya aritmetika modulo) seperti algoritma DSA,RSA, maupun Diffie-Hellman. Variasi algoritma dengan memanfaatkan teori bilangan bulat seperti ini dianggap jauh lebih banyak dan menyulitkan hacker atau pihak yang tidak berkepentingan untuk menyadap data penting yang kita miliki.

Penulis mengambil contoh nomor PIN ATM pada halaman 4 kolom kiri untuk diaplikasikan penyandian dengan algoritma RSA. Perlu diketahui juga bahwa nomor PIN ATM dalam dunia maya direpresentasikan dalam ukuran bit atau kode ASCII untuk karakter huruf, sehingga nomor PIN ATM tersebut dapat ditulis dengan representasi biner untuk nantinya diolah lebih lanjut dengan algoritma RSA. Urutan langkah-langkah algoritma RSA secara garis besar adalah sebagai berikut.

Algoritma RSA [Rinaldi Munir, 2006 (dengan beberapa perubahan)] :

1. Pilih dua buah bilangan prima sembarang, misalkan a dan b. Kerahasiaan dua bilangan ini harus dijaga.
2. Hitung n = a x b. Besaran n tidak dirahasiakan.
3. Hitung m = (a – 1) x (b – 1). Jika bilangan m ini sudah dihitung, hapus a dan b untuk mencegah diketahuinya a dan b oleh pihak lain.
4. Pilih sebuah bilangan bulat untuk kunci publik, misalkan e, yang relatif prima terhadap m.
5. Pilihlah kunci deskripsi misalkan d, yang memenuhi kekongruenan $ed \equiv 1 \pmod{m}$. Lakukan enkripsi terhadap isi pesan dengan persamaan $Ci = Pi^e \bmod n$, yang dalam hal ini Pi adalah blok plainteks dan Ci adalah blok chiperteks. e adalah kunci enkripsi (kunci publik) yang tidak dirahasiakan. Harus dipenuhi persyaratan bahwa nilai Pi terletak di himpunan nilai 0,1,2,.....,n-1 untuk menjamin hasil perhitungan tidak berada di luar himpunan.
6. Proses deskripsi dilakukan dengan menggunakan persamaan $Pi = Ci^d \bmod n$, di mana d adalah kunci deskripsi yang harus dirahasiakan.

Jadi, nomor PIN ATM pada contoh diubah ke dalam bentuk representasi biner, kemudian dipecah ke dalam beberapa blok di mana setiap blok terdiri dari lebih dari 1 byte agar hasil enkripsi lebih rumit. Kemudian, pada setiap blok diberlakukan algoritma RSA dengan urutan langkah-langkah di atas dengan mengkonversi terlebih dahulu setiap blok biner menjadi bilangan biasa. Bilangan enkripsi yang dihasilkan disatukan lagi dengan hasil bilangan enkripsi lainnya sesuai urutan. Kemudian, hasil penggabungan bilangan secara urutan disatukan lagi kemudian dikonversi ke biner sehingga representasi bilangan dari kode biner ‘baru’ yang dihasilkan akan mengaburkan nomor PIN ATM awal. Agar lebih jelasnya, perhatikan bagan di bawah ini :



Penyandian dengan metode seperti pada bagan di atas berlaku pula untuk sandi lewat akun facebook. Bedanya, sandi lewat akun facebook direpresentasikan dahulu dalam kode ASCII karena sandi lewat disusun dalam bentuk rangkaian karakter bukan angka. Kemudian, rangkaian kode ASCII tersebut juga dikonversi ke bentuk desimal untuk selanjutnya diberlakukan lagi algoritma RSA hingga terbentuk rangkaian ASCII yang baru hasil enkripsi dengan algoritma RSA.

Khusus untuk nomor PIN ATM, terdapat algoritma lain yang berguna untuk mengecek keabsahan (keaslian nomor PIN ATM) yang dipakai oleh pengguna. Algoritma ini disebut juga sebagai Algoritma Luhn, ditemukan oleh seorang ilmuwan bernama Hans Peter Luhn. Adapun langkah-langkah algoritmanya dapat ditulis sebagai berikut.

Algoritma Luhn :

1. Kalikan dua setiap nilai untuk setiap digit urutan (posisi) ganjil, menghasilkan nilai Mi untuk setiap posisi ke-(2*i – 1). Jika nilai Mi tersebut ada yang melampaui 9 maka harus dikurangi 9, jika tidak dibiarkan tetap. Kemudian jumlahkan setiap nilai Mi yang didapat dihasilkan nilai N.
2. Jumlahkan semua digit yang ada pada urutan (posisi) genap menghasilkan suatu bilangan O.
3. Jumlahkan nilai N dan O yang didapat lalu cek apakah $(N + O) \equiv 0 \pmod{10}$. Jika memenuhi maka nomor PIN ATM asli. Sebaliknya, jika tidak, maka dapat dipastikan nomor PIN ATM Anda palsu.

Algoritma lainnya yang digunakan dalam proses penyandian data penting seperti akun facebook atau nomor PIN ATM adalah algoritma DSA dan Diffie-Hellman. Algoritma Diffie-Hellman tidak berperan secara langsung dalam proses enkripsi data, namun berperan secara tidak langsung dalam proses pertukaran kunci pribadi antara pengirim dan penerima (agar penyadap tidak mudah menelusuri kunci yang dikirim dari pemilik data ke penerima data). Sedangkan algoritma DSA antara lain berguna dalam hal autentikasi data digital sehingga integritas data yang dimiliki oleh penerima dapat terjamin dengan lebih baik. Algoritma DSA bertujuan untuk memverifikasi identitas pemilik dan penerima pesan dengan cara memberikan identitas berupa kode string atau biner yang menandakan keunikan pesan yang disampaikan. Jadi, setiap pemilik data informasi memiliki dua kunci identitas yang unik satu sama lain. Baik algoritma DSA maupun Diffie-Hellman keduanya memanfaatkan teori bilangan bulat.

Tentunya permasalahan-permasalahan keamanan informasi lainnya seputar dunia maya juga dapat diantisipasi dengan algoritma-algoritma di atas, hanya saja bentuknya mungkin bermacam-macam. Permasalahan lainnya yang relevan untuk topik makalah ini di antaranya transfer rekening secara online, proses jual beli properti secara online, dan masih banyak lagi isu-isu lainnya yang tidak dapat dibahas dalam makalah ini. Intinya, apapun algoritma yang digunakan untuk menjaga keamanan informasi, semuanya harus memenuhi karakteristik kekuatan enkripsi yang baik, artinya harus bisa mengaburkan data atau bahkan memecah data aslinya ke dalam sekian banyak chiperteks sehingga membingungkan pihak penyadap.

IV. ANALISIS

Berdasarkan metode kriptografi yang sudah dipaparkan pada bagian sebelumnya, maka dapat penulis menganalisa beberapa hal berikut :

1. Baik penyandian akun facebook maupun nomor ATM sebenarnya lebih cocok jika menggunakan algoritma yang menerapkan teori bilangan bulat, sebab semakin canggihnya teknologi penyadapan saat ini menuntut kita menggunakan algoritma yang memiliki beberapa kunci yang kompleks (tidak hanya bersifat satu arah saja, melainkan memakai kunci ganda atau bahkan lebih). Di samping itu, dengan algoritma yang mungkin terlihat lebih sederhana dibandingkan dengan algoritma transposisi atau substitusi, hasilnya lebih variatif karena seperti yang sudah diketahui bahwa hasil pemfaktoran bilangan yang besar menghasilkan ribuan banyak kemungkinan kunci dan hal ini semakin membingungkan penyadap yang hendak mencuri data/informasi penting.
2. Meskipun demikian, bukan berarti algoritma klasik seperti Penyandian Caesar, substitusi, dan transposisi tidak cocok dipakai seluruhnya untuk pengamanan akun facebook atau nomor PIN ATM. Kombinasi ketiga algoritma tersebut akan meningkatkan kesulitan kunci enkripsi berkali-kali lipat dibandingkan jika hanya mengandalkan satu algoritma saja. Kombinasi ketiganya juga dapat digabungkan dengan algoritma enkripsi dengan teori bilangan bulat yang lebih mutakhir untuk memperumit kunci enkripsi yang tersedia.
3. Tiap metode enkripsi data mempunyai kelebihan dan kekurangannya masing-masing. Algoritma permutasi yang digunakan dalam metode transposisi sebenarnya memiliki algoritma yang cukup baik bahkan tingkat kesulitannya cukup tinggi. Hanya saja kelemahannya kunci enkripsi hanya bersifat satu arah dan sangat riskan jika sampai bocor ke pihak lain. Selain itu, kesulitan dalam mencarikan kunci deskripsi (kunci balik) juga menjadi faktor yang patut dipertimbangkan kala pemilik data hendak menyampaikan pesan penting ke penerima data. Sedangkan algoritma teori bilangan bulat seperti RSA mempunyai kelebihan kunci ganda yang bersifat dua arah, sehingga jika satu kunci bocor masih ada kunci lain yang bisa dimanfaatkan. Kunci deskripsi maupun kunci enkripsi lebih mudah dicari dalam algoritmanya karena menggunakan satu paket rumus teori bilangan bulat yang lebih mudah dimengerti dibandingkan algoritma klasik. Namun, bukan berarti algoritma yang memanfaatkan teori bilangan bulat juga aman 100 persen dalam pengamanan data karena canggihnya teknologi informasi dan telekomunikasi saat ini.

V. KESIMPULAN

Berdasarkan analisis penulis, dapat disimpulkan bahwa pemilihan algoritma penyandian data untuk keamanan informasi, apalagi di dunia maya, menjadi hal yang penting dan harus didiskusikan lebih lanjut. Penulis menyarankan algoritma yang memanfaatkan teori bilangan bulat dan bilangan prima karena dengan algoritma yang sederhana mampu menghasilkan ribuan macam enkripsi kompleks yang tidak mudah dipecahkan oleh penyadap informasi. Namun, dengan kecanggihan teknologi saat ini, tidak menutup kemungkinan algoritma bilangan bulat dan prima juga bisa dipecahkan. Karena

itu, kombinasi metode enkripsi dengan algoritma bertingkat menjadi solusi terbaik agar keamanan informasi di dunia maya terjamin.

REFERENSI

[1] Adnan, Zainal. *Sistem Penyandian Caesar*. http://kresnapapua07.blogspot.com/2010/10/sistem-penyandian-caesar.html.
Tanggal Akses : 8 Desember 2013, pkl 12.08

[2] Hadiwibowo. *Metode Penyandian Transposisi*. http://hadiwibowo.wordpress.com/2007/03/28/metode-penyandian-transposisi/
Tanggal Akses : 7 Desember 2013, pkl 10.25

[3] Hadiwibowo. *Metode Penyandian Substitusi*. http://hadiwibowo.wordpress.com/2007/04/18/metode-penyandian-substitusi/
Tanggal Akses : 14 Desember 2013, pkl 13.00

[4] http://agorsiloku-sains.blogspot.com/2006/08/mengupas-rahasia-penyandian-informasi.html
Tanggal Akses : 7 Desember 2013, pkl 21.25

[5] http://www.mafiakartukredit.com/2011/07/algoritma-luhn-cek-nomor-kartu-kredit.html
Tanggal Akses : 14 Desember 2013, pkl 21.13

[6] Munir, Rinaldi. 2006. *Diktat Kuliah IF2120 Matematika Diskrit*. Bandung : Program Studi Teknik Informatika STEI ITB

[7] Prastomo, M. Andika. *Aplikasi Kriptografi dengan Algoritma*. http://andikamov.blogspot.com/2013/05/aplikasi-kriptografi-dengan-algoritma.html
Tanggal Akses : 8 Desember 2013, pkl 12.00

[8] Setyoningsih, Astuti. *Sejarah Teori Bilangan*. http://astutisetyoningsih.blogspot.com/p/sejarah -teori-bilangan.html
Tanggal Akses : 7 Desember 2013, pkl 10.00

[9] Windarachma. *Kriptografi Enkripsi dan Steganografi*. http://windarachma079.wordpress.com/2012/01/04/kriptografi-enkripsi-dan-steganografi/
Tanggal Akses : 14 Desember 2013, pkl 12.00

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, 15 Desember 2013

Steve Immanuel Harnadi
13512035