Penggunaan Teori Bilangan dan Kriptografi dalam Peningkatan Keamanan Aplikasi *Personal and Group Messaging*

Verena Severina / 13515047
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13515047@std.stei.itb.ac.id
verenaseverina@gmail.com

***Abstrak*—Semakin banyak orang yang berkomunikasi melalui jaringan internet. Semua orang yang berkomunikasi melalui internet tentu mengharapkan adanya jaminan privasi yang disediakan oleh sarana komunikasi daring yang digunakan. Tetapi, dengan semakin berkembangnya teknologi, semakin banyak juga orang yang berusaha menggunakannya untuk melanggar privasi orang lain dengan menyadap pembicaraan orang lain yang dilakukan secara daring. Jika pembicaraan melalui internet dilakukan sama halnya dengan SMS, maka semua orang akan dapat membaca isi dari pembicaraan tersebut. Hal tersebut dikarenakan SMS merupakan sebuah teks terang yang dapat dibaca oleh semua orang. Dengan menggunakan teori bilangan mengenai kriptografi, maka dapat digunakan metode enkripsi yang dapat digunakan untuk menyembunyikan informasi yang terdapat pada teks terang. Teks terang akan menjadi masukan untuk enkripsi yang akan mengubahnya menjadi teks tersandi (*ciphertext*). Penulis akan membahas bagaimana algoritma *cipher* dapat digunakan untuk meningkatkan keamanan *cyber* dalam berkomunikasi.**

***Kata Kunci*—Cyber Security, Enkripsi, Kriptografi, Teori Bilangan**

I. PENDAHULUAN

Seiring dengan perkembangan teknologi ini, kehidupan manusia memperoleh banyak keuntungan yang dapat memudahkan aktivitas sehari-hari mereka, terutama di bidang informasi. Informasi dapat diakses dengan lebih mudah oleh kalangan manapun. Teknologi informasi semakin berkembang dan membiarkan semua orang untuk dapat memperoleh informasi dengan cepat dan mudah.

Internet merupakan salah satu bentuk teknologi informasi yang digunakan untuk penyebaran informasi. Internet pun menjadi sebuah media penyebaran informasi yang paling digemari dan paling banyak digunakan. Internet menjadi kebutuhan yang sangat penting dalam hidup manusia. Semakin banyak orang yang berlomba-lomba untuk memperoleh informasi secara optimum dengan menggunakan *platform* internet.

Selain untuk memperoleh informasi, internet juga dapat digunakan untuk menyebarkan dan menyimpan informasi. Seringkali, informasi yang hendak disebarkan dan disimpan ini memilik tingkat privasi yang cukup tinggi sehingga pengguna yang menyebarkan informasi ini tentu mengharapkan bahwa yang dapat memperoleh data yang inputnya hanya pihak yang dituju dan tidak siapa pun lagi.

Gambar 1: Salah satu media personal and group messaging *yang tidak menggunakan enkripsi dan dekripsi, sehingga mengirimkan data dalam bentuk teks terang (sumber: http://crillylaw.com.au/wp-content/uploads/2015/09/Email_Subject_Lines.jpg)*

Nyaris semua alat komputasi yang kita gunakan dalam kehidupan sehari-hari berusaha mengembangkan sistem keamanan datanya agar data pengguna dapat terjaga dengan baik dan tidak dapat diakses oleh pihak-pihak yang tidak diinginkan. Salah satu metode untuk mengamankan data tersebut adalah melalui enkripsi.

Enkripsi membiarkan penggunanya untuk menyembunyikan data yang disebarkan dari pihak-pihak yang tidak bersangkutan. Dengan menggunakan enkripsi maka dapat dipastikan bahwa data yang terkirim tetap konfidensial terhadap pihak yang dikirimkan data tersebut.

Enkripsi data tidak hanya digunakan untuk mengirimkan pesan, melainkan dapat digunakan untuk penggunaan hal-hal yang nirkabel, seperti mikrofon nirkabel, interkom nirkabel, telepon genggam, dan lain-lain. Pada dasarnya, enkripsi data dilakukan untuk semua bentuk transfer data yang dilakukan melalui jaringan,

seperti internet, *bluetooth*, dan masih banyak lagi.

Gambar 2: Salah satu aplikasi komunikasi dengan sistem enkripsi dan dekripsi yang paling sulit untuk dihancurkan sekarang ini, WhatsApp Messenger (sumber: http://www.express.co.uk/life-style/science-technology/672960/What-is-WhatsApp-Gold-Secret-Chat-App-Pro-Features)

Meskipun demikian, masih banyak aplikasi dan media komunikasi yang tidak menggunakan metode apa pun untuk menjaga keamanan privasi penggunanya. Salah satu contoh dari kasus ini adalah e-mail dan SMS. Dengan demikian, semua bentuk komunikasi yang dilakukan oleh pengguna dapat dilihat oleh semua pihak yang mau mengaksesnya.

Maka, dibutuhkan pengembangan dari metode enkripsi untuk memastikan semua pengguna dari aplikasi dapat benar-benar menjamin privasinya. Tetapi, apakah enkripsi merupakan metode yang paling baik untuk menyembunyikan data informasi yang disampaikan pengguna? Bagaimana cara kerja enkripsi dalam mengamankan data pengguna dari jangkauan pihak-pihak yang tidak bersangkutan? Apakah semua enkripsi dapat menjamin terjaganya data-data pengguna?

Oleh karena itu, dalam makalah ini, penulis akan membahas mengenai enkripsi yang terdapat dalam berbagai alat komputasi yang menyampaikan informasi melalui jaringan, terutama dalam aplikasi *personal and group messaging*. Dengan demikian, banyak aplikasi *personal and group messaging* yang dapat mengadaptasinya menjadi suatu fitur yang dapat mengembangkan tingkat keamanan dari aplikasi, sehingga privasi dari pengguna dapat terjamin.

II. Teori Bilangan dan Kriptografi

2.1 Teori Bilangan

Teori Bilangan membahas mengenai sifat-sifat dari bilangan bulat dan masalah-masalah yang dapat diselesaikannya. Bilangan bulat adalah bilangan yang tidak memiliki pecahan desimal. Dengan kata lain, bilangan bulat adalah kebalikan dari bilangan riil yang memiliki pecahan desimal.

Dalam bilangan bulat, salah satu sifat yang harus diperhatikan adalah sifat pembagian, terutama pembagian dari bilangan prima. Bilangan prima sendiri memiliki arti bilangan yang hanya habis dibagi oleh 2 bilangan, yaitu dirinya sendiri dan bilangan 1.

Notasi: $x \mid y$

Notasi di samping dapat dibaca sebagai "x habis membagi y" atau "y merupakan kelipatan x" dengan syarat perlu "$y = xz$" dengan z elemen bilangan bulat dan x bukan bilangan 0.

2.2 Aritmatika Modulo

Aritmatika modulo merupakan salah satu operasi aritmatika yang dapat dilakukan kepada bilangan bulat. Aritmatika modulo ini dibutuhkan untuk implementasi pada kriptografi. Pada aritmatika modulo, operator yang digunakan adalah operator "mod". Operator mod memberikan hasil sisa dari pembagian bilangan bulat. Salah satu contoh dari penggunaan operator mod adalah 71 mod 10 = 1. Yang dapat dimengerti sebagai, 71 dibagi dengan 10 menghasilkan nilai = 10, dan memberikan sisa sebesar = 1.

Notasi x mod m = y, dapat diartikan sedemikian sehingga menjadi $x = mz + y$, dengan memastikan bahwa y lebih kecil dari m dan lebih besar sama dengan 0.

Aritmatika modulo ini juga dapat diimplementasikan sebagai sebuah bilangan tak terhingga (x) yang akan digulung dalam sebuah lingkaran yang terbatas (m). Notasi dari implementasi tersebut adalah x mod m.

Dalam aritmatika modulo, terdapat sebuah terminologi yang disebut sebagai kongruen. Operator kongruen adalah "□". Definisi dari kongruen adalah jika x dan y merupakan bilangan bulat dan m merupakan bilangan bulat positif, maka

$a \equiv y \pmod{m}$, jika m habis membagi x dikurangi dengan y.

Oleh karena itu, dalam implementasi aritmatika modulo dengan menggulung sebuah lingkaran terbatas dengan bilangan tak terhingga, setiap kali bilangan melewati titik yang sama pada lingkaran, dapat disimpulkan bahwa kedua bilangan saling kongruen.

2.3 Kriptografi

Kriptografi merupakan salah satu penerapan teori bilangan bulat yang memanfaatkan aritmatika modulo dan juga prinsip bilangan prima. Kriptografi merupakan sebuah ilmu yang digunakan untuk menjaga kerahasiaan dari sebuah pesan dengan menyamarkan pesan menjadi suatu pesan tersandi yang tidak memiliki makna yang signifikan. Pola piker dari kriptografi adalah sebuah pesan hendak disamarkan atau dirahasiakan, maka pesan tersebut akan dienkripsi untuk menjadi sebuah teks *cipher* jika pihak yang dituju memiliki kunci atau metode untuk mengembalikan teks *cipher* maka teks akan didekripsi kembali menjadi teks terang (plainteks).

Gambar 3: bentuk representasi fisik dari proses enkripsi dan dekripsi (sumber: http://www.b1router.com/en/encryption/)

Teks *cipher* merupakan sebuah teks yang tidak rahasia dan dapat diakses oleh siapa saja namun tidak memiliki makna rahasia yang dimaksudkan oleh pengirim pesan. Jika penerima pesan memilik kunci dari teks *cipher*, maka pesan dapat dikembalikan menjadi plainteks.

Kriptografi telah ada semenjak zaman dahulu kala dan awalnya digunakan sebuah alat yang disebut sebagai *scytale*.

Gambar 4: scytale *yang digunakan untuk mentrasposisikan pesan (sumber: https://id.wikipedia.org/wiki/Berkas:Skytala%26EmptyStrip-Shaded.png)*

Alat ini merupakan sebuah pita panjang dengan pesan yang terkandung di dalamnya. Pita ini dililitkan pada sebuah batang silinder. Untuk membaca pesan ini maka sang penerima harus melilitkan pita tersebut kembali sebuah batang silinder yang memiliki diameter yang sama dengan diameter dari silinder sang pengirim pesan.

Notasi dari enkripsi E yang memetakan sebuah pesan P menjadi teks *cipher* C adalah sebagai berikut.

$$E(P) = C$$

Sementara notasi dari proses enkripsi D yang mengembalikan sebuah teks *cipher* C menjadi plainteks P dapat dituliskan sebagai berikut.

$$D(C) = P$$

Dan fungsi ini akan memenuhi persamaan berikut.

$$D(E(P)) = P$$

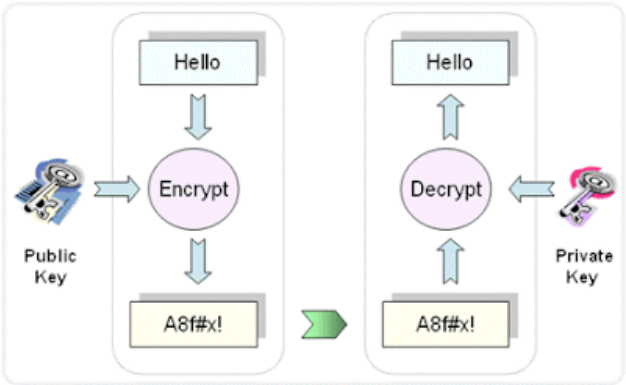
Algoritma kriptografi atau *cipher* merupakan fungsi yang berguna untuk proses enkripsi dan deskripsi pesan. Suatu algoritma kriptografi dapat dinilai lebih kuat jika kerja yang dibutuhkan untuk memecahkan sebuah teks *cipher* kembali menjadi sebuah plainteks. Semakin banyak kerja yang dibutuhkan untuk memecahkan suatu sandi, berarti semakin lama waktu yang dibutuhkan. Hal tersebut mengindikasikan bahwa suatu algoritma semakin aman dan kuat untuk digunakan menyandikan sebuah pesan.

Sekarang ini, algoritma dari proses enkripsi dan dekripsi tidak lagi menjadi penentu dari kekuatan sebuah proses enkripsi dan dekripsi. Melainkan kekuatan kriptografi ditentukan dari kunci yang menjaga kerahasiaan dari sebuah pesan. Kunci ini berlaku sebagai sandi lewat yang digunakan untuk mengenkripsi dan mendekripsi.

Oleh karena itu, dengan mengandalkan pada kekuatan kuncinya, maka akan dibutuhkan 2 jenis kunci yaitu kunci untuk mengenkripsi (misal: K1) dan kunci untuk mendekripsi (misal: K2).

Jika kunci untuk enkripsi dan dekripsi pesan adalah sama (K1 = K2), maka algoritma ini disebut sebagai algoritma simetri. Pada algoritma simetri, kedua kunci baik untuk enkripsi maupun dekripsi harus dirahasiakan dari semua orang kecuali pengirim dan penerima pesan.

Sementara untuk kebalikannya, algoritma dengan kunci untuk enkripsi dan dekripsi pesan yang berbeda (K1 ≠ K2) disebut sebagai algoritma nirsimetri. Pada algoritma ini terdapat kunci publik "*public key*" yang tidak dirahasiakan dan kunci pribadi "*private key*" yang dirahasiakan. Salah satu contoh dari algoritma nirsimetri ini adalah algoritma RSA (Rivest-Shamir-Adleman), Triple DES (Data Encryption Standard), AES (Advanced Encryption Standard), Twofish, dan lain-lain.



Gambar 5: representasi dari private key *dan* public key *(sumber: http://hacksandtrickz.blogspot.co.id/2011/08/hack-simple-encryption-decryption.html)*

III. METODOLOGI

3.1 Penentuan Kunci Publik dan Privat

Algoritma yang digunakan untuk menentukan kedua jenis kunci ini dapat menjadi beragam. Dalam makalah ini, penulis akan menggunakan algoritma RSA.

1. Memilih 2 bilangan prima sembarang. Kedua bilangan ini harus dirahasiakan.

$$a = 17$$
$$b = 31$$

2. Menghitung n = a x b. Nilai n tidak dirahasiakan.

$$n = a \times b$$
$$n = 17 \times 31$$
$$n = 527$$

3. Menghitung m = (a – 1) x (b – 1). Kemudian membuang a dan b agar nilai kedua bilangan tidak diketahui oleh pihak yang tidak bersangkutan.

$$m = (a - 1) \times (b - 1)$$
$$m = (17 - 1) \times (31 - 1)$$
$$m = 16 \times 30$$
$$m = 480$$

4. Memilih bilangan bulat (e) untuk *public key* yang relatif prima terhadap m.

$$e = 7$$

5. Membangkitkan nilai kunci untuk dekripsi (d).

$$ed \equiv 1 \pmod{m}$$
$$d = 343$$

6. Melakukan enkripsi terhadap pesan yang ingin disampaikan dengan persamaan berikut.

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

dengan p_i sebagai pesan yang ingin disampaikan dan c_i sebagai pesan yang telah diubah.

7. Melakukan proses dekripsi dengan persamaan berikut.

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

3.2 Tambahan dari Algoritma

Algoritma sesuai yang telah dibentuk di atas telah dibuktikan untuk menjadi tidak seaman sebagaimana yang diperkirakan. Oleh karena itu dibutuhkan beberapa penambahan yang dapat dilakukan terhadap algoritma itu sehingga dapat memenuhi kebutuhan masyarakat dunia sekarang yang membutuhkan media komunikasi yang aman dan dapat menjaga privasi masing-masing orang.

Bentuk enkripsi yang umum digunakan sekarang ini adalah sebagai berikut.

1. Pesan yang dirahasiakan dikirim oleh pengirim pesan
2. Pesan dienkripsi dengan *public key*
3. Pesan yang telah dienkripsi masuk ke dalam server perusahaan penyedia *platform personal and group messaging*
4. Di dalam server, pesan akan didekripsi dan disimpan dalam server perusahaan yang bersangkutan
5. Pesan kembali dienkripsi dan dikirim ke penerima pesan
6. Pesan diterima oleh penerima dan kembali didekripsi

Metode tersebut banyak digunakan oleh media sosial seperti Facebook. Dengan menggunakan metode tersebut maka orang di dalam perusahaan penyedia *platform* dapat mengakses pesan yang dikirimkan oleh pengguna. Pesan tersebut juga dapat diakses oleh pemerintah, atau perusahaan tersebut dapat dibajak dan kemudian semua data pesan yang telah mereka simpan dalam server mereka dapat dilihat dan diperoleh oleh pihak-pihak yang tidak diinginkan.

Modifikasi pada algoritma dapat dilakukan dengan melakukan enkripsi *end-to-end*. Enkripsi ini merupakan sebuah bentuk enkripsi di mana yang memegang kunci untuk mendekripsi dan mengenkripsi pesan disimpan pada *device* yang dimiliki oleh pengguna, sebagaimana yang telah dilakukan oleh WhatsApp Messenger.

Dengan demikian, tidak ada yang dapat mengakses pesan selain dari sang pengirim dan penerima pesan. Kunci dekripsi tidak disimpan pada server perusahaan sehingga pada saat pesan yang dirahasiakan masuk ke dalam sistem perusahaan dan tersimpan di dalamnya, pesan tidak akan didekripsi dan akan dibiarkan dalam bentuk yang sudah terenkripsi sampai dikirim ke *device* penerima, setelah itu melalui *private key* yang dimiliki oleh *device* penerima, maka pesan dapat didekripsi.

Enkripsi *end-to-end* dapat menjamin bahwa kunci dekripsi tidak pergi meninggalkan *device* pengirim pesan. Oleh karena itu, tidak ada yang dapat mengakses pesan yang terkirim, termasuk orang-orang yang ebekrja di perusahaan penyedia media komunikasi tersebut.

Hal lain yang ditambahkan dari algoritma tersebut adalah pemilihan bilangan prima yang lebih kompleks. Algoritma tersebut dapat dikembangkan sehingga menerima input berupa karakter lain yang tetap bernilai prima. Semakin sulit dan kompleks bilangan prima yang dipilih maka akan semakin sulit bilangan tersebut untuk ditembus dari pihak luar yang tidak bersangkutan dengan pesan yang ingin dirahasiakan tersebut.

Selain itu langkah lain yang dapat dilakukan adalah menambahkan jumlah *private key* yang perlu dimiliki oleh penerima pesan dan ditembus oleh pihak yang tidak bersangkutan. Pada kasus yang ideal, orang yang mempunyai *private key* akan memiliki kompleksitas algoritma yang linear. Sementara orang yang tidak memiliki akses berupa *private key* akan memiliki waktu kompleksitas algoritma sebesar 2^k dengan k sebagai panjang dari kunci yang dibutuhkan.

Kunci privat dapat ditambahkan ke dalam setiap akun pengguna ketika pengguna pertama kali mendaftar dalam *platform* komunikasi tersebut. Selain itu, untuk menambahkan keamanan dalam setiap pesan, telepon,

gambar, pesan suara, video, dan lain-lain dapat di-*generate* sebuah kunci enkripsi yang digunakan untuk masing-masing data yang dikirimkan.

IV. Studi Kasus

Salah satu contoh dari studi kasus yang dapat digunakan adalah salah satu kejadian yang baru saja terjadi pada tahun 2016 ini. FBI menginstruksikan Apple untuk masuk ke dalam iPhone yang merupakan milik dari Syed Farook, salah satu orang yang terlibat dalam serangan teroris di San Bernadino, California. Apple dan FBI terus mendebatkan mengenai privasi dan keamanan yang dapat dilanggar oleh pihak yang memiliki otoritas untuk membuka akses dari iPhone tersebut.

Gambar 6: Terjadi perselisihan antara Apple dan FBI (sumber: http://www.trustedreviews.com/opinions/apple-government-letter-san-bernardino-encryption)

Tanpa adanya penerima algoritma enkripsi yang sesuai maka banyak pengguna dari media sosial yang akan terganggu privasi dan keamanannya. Karena jika perusahaan yang menyediakan *platform personal and group messaging* dapat mengakses data dari penggunanya, tidak dapat dipastikan bahwa pihak-pihak luar yang hendak menggunakan data pengguna untuk niat jahat pun tidak dapat dihentikan.

Untuk memperoleh kepercayaan dari warga dan para pengguna dari seluruh dunia, maka perusahaan yang menjadi *platform* dari *personal and group messaging* harus meningkatkan sistem enkripsinya. Karena jika semua orang dapat mengakses data dan pesan yang digunakan oleh pengguna *platform* tersebut, sama halnya dengan jika pengguna menggunakan SMS maupun surat elektronik yang tidak menggunakan sistem enkripsi maka orang akan menghindari untuk menggunakan aplikasi *personal and group messaging* tersebut dan menggunakan aplikasi lainnya untuk mendapatkan jaminan privasi yang lebih terjamin.

V. Kesimpulan

Teori bilangan dan penggunaan kriptografi sangat dibutuhkan dalam peningkatan keamanan dalam *personal and group messaging*, melalui metode enkripsi dan dekripsi pesan, gambar, video, dan semua bentuk data yang dikirimkan oleh pengguna. Metode enkripsi merupakan cara menyembunyikan data pengguna yang paling baik yang dapat digunakan sekarang ini. Penggunaaan *key* yang lebih terstruktur dan kompleks dapat membuat data pengguna menjadi sangat aman dan sangat sulit untuk ditembus. Tetapi harus diperhatikan jika terjadi galat yang dilakukan oleh manusia yang menyusun algoritma. Penggunaan metode enkripsi yang paling baik adalah dengan enkripsi *end-to-end*.

VI. Ucapan Terima Kasih

Saya mengucapkan terima kasih kepada Tuhan Yesus, atas segala berkatnya yang membiarkan saya untuk menulis makalah ini. Puji Tuhan saya haturkan jika makalah saya ini dapat diselesaikan dengan hasil yang baik dan maksimal. Saya mengucapkan terima kasih kepada Bapak Rinaldi dan Ibu Harlili sebagai dosen mata kuliah Matematika Diskrit. Saya juga mengucapkan terima kasih untuk keluarga serta semua teman-teman saya yang terus mendukung saya dalam kuliah ini.

Referensi

[1] Kenneth H. Rosen, *Discrete Mathematics and Its Application.* 7th Edition. New York: McGraw-Hill, 2012.

[2] Rinaldi Munir, *Diktat Kuliah IF2120: Matematika Diskrit.* Bandung: Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung, 2006.

[3] http://www.makeuseof.com/tag/encryption-care/ style—Submitted for publication)," *IEEE J. Quantum Electron.*, submitted for publication.

[4] http://www.pcadvisor.co.uk/feature/internet/whatsapp-what-is-end-to-end-encryption-opt-out-of-adverts-3637780/B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.

[5] https://www.quora.com/How-secure-is-WhatsApps-new-end-to-end-encryption

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

Verena Severina - 13515047