Penerapan Algoritma Modulo dan Bilangan Prima dalam Algoritma Kriptografi Rivest-Shamir-Adleman (RSA)

Firman Rickson Saragih
13506096
1) Jurusan Teknik Informatika ITB, Bandung, email: if16096@students.if.itb.ac.id

Abstract – *Salah satu bidang yang memanfaatkan algoritma modulo dan bilangan prima secara meluas adalah bidang kriptografi. Kerahasiaan data sangat diperlukan dalam hal komunikasi data.Untuk menjamin keamanan dan kerahasiaan data tersebut diperlukan teknik tertentu untuk menyandikan data atau informasi yang disebut kriptografi. Ada berbagai jenis algoritma kriptografi seperti DES, RSA dan sebagainya yang berusaha untuk menciptakan suatu algoritma yang benar-benar dapat mengamankan data atau informasi yang ditransmisikan. Untuk itu para kriptografer semakin lama semakn berusaha menciptakan algoritma yang rumit untuk lebih menjamin keamanan informasi yang dienkripsikan. Namun sebenarnya semakin sederhana algoritma pengenkripsian yang dibuat akan semakin baik, karena dengan demikian proses komputasinya akan semakin sedikit sehingga akan memakan waktu lebih sedikit untuk mengeksekusinya.*

*Makalah ini akan membahas salah satu bentuk kriptografi modern yang sampai dengan pembuatan makalah ini masih merupakan algoritma kriptografi yang "mustahil "untuk dipecahkan yaitu kriptografi Rivest-Shamir-Adleman (*RSA)

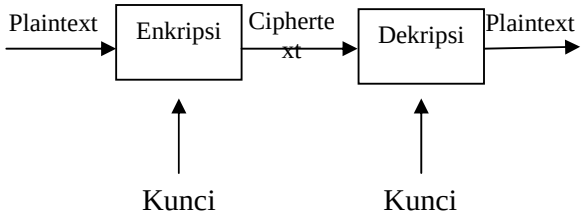
Kata Kunci*: algoritma, bilangan prima, enkripsi, dekripsi, kerahasiaan data, key, kriptografi, modulo, RSA,*

1. PENDAHULUAN

Suatu instansi atau organisasi sangat membutuhkan keamanan infrastruktur teknologi informasi yang baik untuk melindungi aset-asetnya terutama informasi-informasi dan data-data yang penting dan sensitif. Sehingga saat ini dibutuhkan system keamanan yang lebih kompleks dengan kesanggupan untuk mengikuti perkembangan yang ada agar dapat melindungi system dari berbagai ancaman yang mungkin timbul.

Salah satu cara yang digunakan untuk menjamin keamanan dari infrastruktur teknologi adalah dengan menjamin keamanan komunikasi. Komunikasi yang aman dimaksudkan untuk melindungi data ataupun informasi ketika dikirimkan atau ditransmisikan kepada pihak lain, sehingga data atau informasi yang ditransmisikan itu tidak dapat disadap dimanipulasi ataupun dirusak oleh pihak-pihak yang tidak bertanggungjawab. Salah satu cara untuk mengamankan komunikasi adalah dengan menerapkan teknik penyandian/ kriptografi.

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Pesan yang dirahasiakan dalam kriptografi disebut plainteks (plaintext) dan hasil penyamaran disebut chiperteks (chipertext). Proses penyamaran dari palinteks ke chiperteks disebut enkripsi (dari kata encryption) dan proses pembalikan dari chiperteks menjadi plainteks kembali disebut dekripsi (decryption). Baik proses enkripsi maupun proses dekripsi melibatkan satu atau beberapa kunci kriptografi. Dalam suatu system di mana terdapat algoritma kriptografi, ditambah seluruh kemungkinan plaintext, ciphertext dan kunci-kuncinya disebut kriptosistem (cryptosystem atau cryptographic system) Proses tersebut dapat digambarkan secara sederhana sebagai berikut :



Gambar 1.Enkripsi/Dekripsi Sederhana

Ada banyak jenis metode kriptografi yang umum digunakan. Salah satu metode kriptografi yang tertua adalah dengan menggunakan scytale yang digunakan oleh tentara Sparta di Yunani pada permulaan tahun 400 SM [1]. Alat ini merupakan sebuah pita panjang dari daun papyrus yang dililitkan pada sebatang silinder. Pesan yang akan dikirmkan ditulis secara horizontal, kemudian pita dilepas. Untuk dapat membaca pesan itu kembali, orang yang menerima pesan harus melilitkan kembali pita tersebut pada silinder yang diameternya sama dengan silinder yang dipergunakan pengirim pesan tersebut. Teknik kriptografi ini disebut metode transposisi yang merupakan metode enkripsi tertua.

Pada zaman modern, manusia tidak henti-hentinya berusaha menemukan cara-cara baru untuk menjamin keamanan dan kerahasiaan informasi yang dimiliki atau disebarluaskan. Salah satu perkembangan yang cukup signifikan dalam perkembangan algoritma kriptografi di zaman modern adalah perkembangan algoritma kriptografi dengan sistem *public key* atau kriptografi dengan kunci publik yang tidak dirahasiakan. Salah satu jenis algoritma kriptografi yang tergolong ke dalam jenis ini adalah algoritma Rivest-Shamir-Adleman (RSA) yang menggunakan algoritma modulo dalam proses enkripsi dan dekripsinya.

Penggunaan algoritma modulo dalam pengenkripsian dan pendekripsian informasi sebenarnya cukup rumit, namun perkembangan kriptografi ke arah ini didorong pula oleh perkembangan teknologi di bidang komputer. Karena komputer dapat mengerjakan proses komputasi yang sebelumnya dianggap rumit dalam waktu yang relatif singkat Kemunculan dari algoritma jenis ini juga dipengaruhi oleh perlunya satandardisasi dalam pengenkripsian dan pendekripsian informasi. Karena semakin banyak orang awam yang membutuhkan kriptografi baik di bidang bisnis maupun bidang-bidang lainnya. Sehingga orang tidak dpata lagi menggunakan metode kriptografi yang *private* untuk golongan sendiri saja. Perkembangan ini mendorong timbulnya algoritma kriptografi yang disebut DES yang cukup kuat dan sulit ditembus oleh kriptanalis, namun algoritma ini memiliki beberapa kelemahan, di antaranya adalah pendistribusian *key*. Jika dua pihak ingin berkomunikasi dengan aman, kedua pihak yang menggunakan algoritma DES harus bergantung pada pihak ketigauntuk men-*deliver key*, dan hal ini merupakan *link* yang paling lemah dalam algoritma kriptografi ini. Dalam dunia bisinis dilema yang dihadapai cukup berat yaitu jumlah biaya yang besar untuk memastikan pengiriman *key* yang cukup aman, terutama jika perusahaan tersebut memiliki banyak cabang yang tersebar di seluruh dunia.

Dilema tersebut memicu timbulnya *public key cryptography* sebagai metode yang dpat menyelesaikan maslah pendistribusian *key*. *Public key cryptography* muncul dengan dilatarbelakangi penemuan kunci asimetrik, yakni kunci enkripsi yang berbeda dengan kunci dekripsi. Secara sederhana hal ni dapat digambarkan dengan kunci gembok (*padlock*), setiap orang dapat mengunci gembok tersebut, namun hanya orang yang memiliki kunci saja yang dapat membukanya. Penemuan *key* asimetrik ini oleh Whitfield merupakan gebrakan baru dalam dunia kriptografi karena sebelumnya algoritma kriptografi yang ada selalu menggunakan prinsip simetrik (kunci pengenkripsi sama dengan pendekripsi), dan merupakan cikal bakal munculnya *public key cryptography* dan algoritma RSA.

2. PEMBAHASAN

Prinsip penggunaan algoritma RSA dalam kriptografi data adalah sebagai berikut :

1. A menciptakan sebuah *public key* yang kemudian dipublikasikan agar semua orang yang akan mengirim pesan kepadanya dapat mengenkripsikan pesan dan data yang akan dikirimkan tersebut terlebih dahulu. Karena *public key* merupakan *one way function* maka adalah mustahil bagi orang lain untuk membalik (*reverse*) prosesnya dan mendekripsikan pesan yang dikirmkan tersebut.
2. Orang yang menciptakan *public key* tersebut kemudian dapat mendekripsikan pesan tersbut dengan menggunakan *private key* yang dimilikinya sendiri. Sehingga dengan menggunakan algoritma ini hanya A sajalah yang dapat mendekripsikan pesan-pesan dan data-data yang dikirimkan kepadanya.

Inti dari sistem ini adalah suatu fungsi searah (*one-way function*) yang didasarkan pada semacam fungsi modulo.Metode pengenkripsian dan pendekripsiannya adalah sebagai berikut :

1. Dipilih 2 bilangan prima yang cukup besar, yaitu *p* dan *q*. Kedua bilangan prima ini harus dirahasiakan nilainya.
2. Kedua bilangan prima p dan q tadi kemudian dikalikan menjadi suatu bilangan N. Kemudian dipilih sebuah bilangan lain yang relatif prima terhadap (p-1) dan (q-1), sebut saja e.
3. Nilai e dan N kemudian dapat dipublikasikan kepada siapapun yang akan mengirimkan data atau pesan ke orang yang bersangkutan. Kedua nilai N dan e ini disebut *public key*, nilai e antara 2 pihak yang berbeda mungkin saja sama namun setiap orang sebaiknya memiliki nilai N yang berbeda-beda tergantung pada nilai p dan q yang dipilihnya.
4. Untuk mengenkripsikan sebuah pesan, pesan tersebut harus diubah terlebih dahulu menjadi sebuah bilangan M. Misalnya sebuah kata dapat diubah menadi ASCII dan kode ASCII tersebut kemudian dienkripsikan. M kemudian dienkripsikan menjadi *ciphertext* C denga rumus :
   $$C = M^e \ (mod\ N)$$
5. Misalkan dikirimkan sebuah abjad tunggal X. Dalam ASCII direpresentasikan oleh sebuah bilangan 1011000 yang ekivalen dengan bilangan 88 pada basis 10.
6. Misalkan p = 17 dan q = 11, maka N = 187. Kemudian dipilih e = 7. Maka nilai C dapat dihitung $C = 88^7 \pmod{187}$ dan diperoleh

ciphertext C = 11.

7. Eksponensial pada aritmatika modulo adalah fungsi searah (*one way function*) sehinga adalah sangat sulit untuk bergerak mundur dari C dan memperoleh pesan aslinya.
8. Namun pemilik *private key* dapat dengan mudah mendekripsi pesan tersebut karena ia telah mengetahui nilai p dan q. Dari nilai p dan q tersebut kemudian dapat dihitung nilai d, atau disebut juga kunci dekripsi, yang berfungsi sebagai *private key* bagi yang bersangkutan. Nilai d dapat dihitung dengan menggunakan rumus sebagai berikut :

   $$e \times d = 1 \ (mod (p-1) \times (q-1))$$
9. Dalam contoh sebelumnya maka C (11) dapat didekripsi dengan menggunakan d sbb :
   7 x d = 1 (mod (17-1) x (11-1))
   7 x d = 1 (mod 16 x 10)
   7 x d = 1 (mod 160)
   d = 23
   Menghitung nilai d dapat dilakukan dengan algoritma Euclidean.
10. Dengan menggunakan d = 23 maka C dapat didekripsi dengan rumus

    $$M = C^d \ (mod\ N)$$

    Sehingga,
    $M = 11^{23}$ (mod 187)
    Diperoleh M = 88.

Metode ini memungkinkan setiap orang untuk mengenkripsikan pesan untuk orang tertentu menggunakan nilai N, tetapi hanya penerima pesan tersebut yang dapat mendekripsikan pesan tersebut, karena penerima pesan adalah orang satu-satunya yang mengetahui nilai p dan q.

Dalam algoritma ini N sangat penting karena N merupakan komponen yang fleksibel dalam fungsi searah, yang artinya setiap orang dapat memilih nilai N yang berbeda-beda. Nilai N yang dipilih menjadi *public encryption key* dan dapat dipublikasikan dengancara apapun dan edia apaun dan kepada siapapun. Dan siapapun yang ingin mengirim pesan kepada orang tersebut dapat mencari nilai N dan mengenkripsikan pesan sebelum mengirimkannya, sedangkan kerahasiaan pesan itu sendiri dapat dijamin karena hanya si penerima pesan saja yang dapat mengartikan kembali pesan tersebut.

Untuk membayangkan sulitnya memecahkan algoritma RSA, dapat diambil contoh dari sudut pandang seorang pembajak pesan. Misalnya B memiliki *public key* N = 408.508.091 yang dipublikasikan. C mengirimkan pesan kepada B dengan menggunakan *public key* tersebut, akan tetapi di tengah jalan, pesan tersebut dapat dibajak oleh D. Satu-satunya cara bagi D untuk mendekripsikan pesan tersebut adalah dengan membalik *one way encryption function*, D memiliki *public key* N namun tidak mengetahui nilai p dan q milik B. D kemudian harus berusaha menurunkan nilai p dan q milik b dengan mencari-cari nilai bilangan mana yang jika dikalikan akan memperoleh nilai 408.508.091, dengan menggunakan proses faktorisasi. Proses faktorisasi merupakan proses yang memakan waktu cukup lama. Ada berbagai macam cara yang dapat digunakan untuk mencari faktor prima dari suatu bilangan, namun pada dasranya semua cara tersebut melibatkan pengecekan setiap bilangan prima untuk melihat apakah N dapat dibagi dengan bilangan tersebut tanpa sisa. Jika D memiliki sebuah kalkulator dan dapat mengecek 4 faktor berupa bilangan prima dalam semenit, maka D akan membutuhkan 500 menit untuk mencari p dan q atau kira-kira 8 jam.

Untuk meningkatkan keamanan algoritma RSA, para pengguna algoritma ini menggunakan bilangan-bilangan prima yang makin besar. Misalnya dengan memilih bilangan prima dengan besar kira-kira 10^{65} akan menghasilkan bilangan N sebesar kira-kira 10^{65} x 10^{65} yaitu 10^{130}. Untuk memperoleh hasil perkalian dari dua bilangan tersebut sebuah komputer dapat menghitung dalam waktu yang relatif singkat, akan tetapi untuk mencari faktor prima dari keduanya, komputer yang cukup cepat pun akan memerlukan waktu bertahun-tahun untuk memfaktorkannya dan mencari nilai p dan q. Sehingga dengan nilai p dan q yang cukup besar algoritma RSA dapat dikatakan “tak tertembus”.

Satu-satunya masalah yang dihadapi oleh algoritma kriptografi Rivest-Shamir-Adleman ini adalah jika suatu saat di masa depan ditemukan suatu algoritma pemfaktoran yang luarbiasa mangkus dan cepat. Mungkin saja dalam beberapa waktu ke depan, ada seseorang yang menemukan cara yang cepat untuk memfaktorkan N. Namun selama ini, banyak pakar matematika yang berusaha untuk menemukan cara yang cepat untuk memfaktorkan, akan tetapi algoritma pemfaktoran tetap merupakan algoritma yang rumit dan sangat menghabiskan waktu. Sebagian besar ahli matematika beranggapan bahwa pemfaktoran adalah hal yang sangat sukar dan ilmu matematika sepertinya tidak menunjukkan adanya jalan pintas untuk ditemukan.

Faktor lain yang menghambat penggunaan algoritma RSA secar meluas pada zaman sekarang adalah dilema keamanan. Suatu algoritma pengenkripsian yang mangkus, sangkil dan aman dapat saja digunakan oleh pihak-pihak yang tidak bertanggung jawab seperti teroris, sehingga penggunaannya dalam pengiriman pesan akan menimbulkan bahaya bagi keamanan masyarakat karena pihak pemerintah dan keamanan akan kesulitan dalam menangani permasalahan-permaslahan yang ditimbulkan oleh pihak teroris tersebut.

Algoritma RSA pertama kali diumumkan pada bulan Agustus tahun 1977, saat Martin Gardner menulis artikel berjudul “A New Kind of Cipher that Would Take Millions of Years to Break” (Suatu Jenis Sandi Baru yang Membutuhkan Jutaan Tahun untuk Dipecahkan) pada kolom “Mathematical Games” di *Scientific American*. Setelah menjelaskan mengenai *public key cryptography* Gardner membuat sayembara untuk para pembacanya. Ia memuat sebuah cipherteks dan sebuah public key N yang digunakan untuk mengenkripsinya. N = 114.381.625.757.888.867.669.235.779.976.146.612.0 10.218.296.721.242.362.562.561.842.935.706.935.24 5.733.897.830.597.123.563.958.705.058.989.075.147. 599.290.026.879.543.541
Gardner kemudian menantang para pembaca untuk mendekripsi cipherteks tersebut dengan hadiah sebesar $ 100.
Sayembara tersebut baru terpecahkan 17 tahun kemudian, pada tanggal 26 April 1994, oleh sebuah tim yang terdiri dari 600 sukarelawan, yang berhasil menemukan nilai p dan q kemudian mendekripsikan cipherteks tersebut, yang ternyata merupakan sejumlah angka yang bila diterjemahkan merupakan kalimat “the magic words are squeamish ossifrage”. Sukarelawan yang menyelesaikan sayembara tersebut berasal dari berbagai negara, seperti Australia, Inggris Raya, Amerika Serikat dan Venezuela, setiap sukarelawan mengerjakan satu bagian dari problem tersebut pada waktu luang masing-masing di komputer masing-masing. [2]

Hal ini menunjukkan sulitnya memecahkan algoritma RSA menggunakan algoritma pemfaktoran yang ada sekarang. Sayembara Gardner menggunakan bilangan N yang berorde 10^{129}. Sementara pada zaman sekarang, para pengguna algoritma kriptografi RSA biasanya menggunakan nilai yang bahkan jauh lebih besar dari nilai N yang digunakan Gardner untuk menjamin kerahasiaan dan keamanan data, sehingga bahkan komputer tercepat saat ini pun akan membutuhkan waktu yang sangat lama untuk memfaktorkan bilangan tersebut dan memperoleh nilai p dan q.

3. KESIMPULAN

Penggunaan algoritam kriptografi yang baik sangat dibutuhkan dalam kehidupan di zaman modern untuk memastikan kerahasiaan dan keamanan dari suatu data yang dikirimkan.

Algoritma kriptografi telah berkembang dari zaman dahulu hingga sekarang, mulai dari kriptografi transposisi hingga yang paling mutakhir yaitu *public key cryptography* yang salah satu jenisnya adalah RSA.

Kemunculan *public key cryptography* ditimbulkan pada awalnya oleh keinginan akan adanya standardisasi kriptografi. Kebutuhan akan standardisasi ini memunculkan algoritma DES yang sangat aman untuk mengenkripsikan data. Akan tetapi algoritma ini ternyata memiliki kelemahan yang cukup signifikan yaitu kesulitan dalam pendistribusian *key* dan menjamin keamanan pendistribusian *key* tersebut agar tidak jatuh ke tangan pihak-pihak yang tidak bertanggungjawab.

Kelemahan dari algoritma tersebut memunculkan ide *assymmetric cryptography* yang memiliki kunci berbeda untuk mengenkripsi dan mendekripsi. Ini merupakan cikal bakal ditemukannya RSA sebagai suatu jenis *public key cryptography* yang memungkinkan setiap orang untuk mengenkripsikan tetapi hanya mengizinkan pemilik *private key* saja yang dapat mendekripsikan data itu ke bentuk semula.

Keuntungan dari menggunakan algoritma RSA adalah meungkinkan untuk mempublikasikan *public key* kepada siapapun sehingga seseorang dapat menerima pesan cipherteks dari siapapun, namun demikian keamanan tetap terjamin karena yang dapat menerjemahkan kembali cipherteks tersebut hanya si penerima pesan yang memiliki *private key.*

Keuntungan lain dari penggunaan algoritma RSA adalah algoritma ini sangat sulit untuk dipecahkan, karena keterbatasan algoritma pemfaktoran yang ada saat ini. Tingkat keamanan algoritma ini juga dapat ditingkatkan dengan penggunaan nilai p dan q yang sangat besar. Dengan demikian, komputer tercepat sekalipun akan memerlukan waktu yang sangat lama untuk mencari nilai p dan q dari *public key* yang dipublikasikan.

Kemanan algoritma RSA sebenanya sepenuhnya bergantung pada adanya algoritma yang cukup cepat untuk memfaktorkan atau mencari faktor prima dari suatu bilangan yang besar. Jika suatu saat telah ditemukan algoritma baru yang jauh lebih cepat dari algoritma yang ada sekarang dalam menemukan faktor prima dari suatu bilangan yang besar, maka niscaya algoritma RSA akan dengan mudah dipecahkan . Namun karena belum ditemukannya algoritma yang demikian maka sampai sekarang algoritma RSA tetap dianggap sebagai metode kriptografi yang terkuat dan teraman.

.

DAFTAR REFERENSI

[1] Rinaldi Munir, Struktur Diskrit", 2008,

[2] Simon Singh, "The Code Book : The Science of Secrecy from Ancient Egypt to Quantum Cryptogrphy", *Anchor Books*, 1999, New York, USA, pp.262-279.