Analisis dan Modifikasi *Multiplicative Group* Pada Algoritma ElGamal

Meirza Auriq – NIM : 13504103
Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10Bandung,
Email: if14103@students.if.itb.ac.id

Abstract *– Algoritma ElGamal merupakan algoritma enkripsi kunci asimetris untuk kriptografi kunci publik yang didasari kesepakatan kunci Diffie-Hellman. Algoritma ini ditemukan oleh ilmuan Mesir, Taher ElGamal, pada tahun 1984. Keamanan algoritma ini terletak pada kesulitan dalam memecahkan masalah logaritma diskrit. Algoritma ElGamal terdiri dari tiga komponen, yaitu pembangkit kunci (key generator), algoritma enkripsi, dan algoritma dekripsi.*
Algoritma ElGamal bekerja menggunakan kumpulan nilai GF(p) yang berulang (multiplicative group of GF(p)), dan di dalam kasus ini, proses logaritma diskrit mengharuskan pengguna untuk terus memperbesar modulus bilangan prima p dengan tujuan menambah keamanan. Akan tetapi, tugas untuk mendapatkan kumpulan nilai GF(p) yang berulang bukanlah hal yang mudah dilakukan untuk pengguna biasa. Hal ini dapat ditanggulangi dengan melakukan skema algoritma ElGamal menggunakan kumpulan nilai GF(p^m). Oleh karena itu, akan dilakukan modifikasi sehingga algoritma ElGamal dapat bekerja menggunakan kumpulan nilai GF(p^m) yang berulang, subgroup dari kumpulan nilai GF(p^m) dan sebuah sistem aljabar yang dinamakan kumpulan nilai palsu GF(p^m) yang berulang (spurious multiplicative group of GF(p^m)).
Hasil modifikasi menunjukkan bahwa algoritma enkripsi kunci-publik ElGamal berdasarkan kumpulan nilai GF(p^m) yang berulang, subgroup dari kumpulan nilai GF(p^m) mudah untuk digunakan dan penggunaan nilai palsu GF(p^m) yang berulang (SMG(p^m)), yang menjadikan kriptosistem lebih tidak dapat diperkirakan dan menambah besar kunci

Kata Kunci*: Kriptografi kunci-publik, algoritma ElGamal, multiplicative group.*

1 PENDAHULUAN

1.1 Latar Belakang

Kriptografi modern merupakan algoritma kriptografi yang berkembang pada zaman modern ini. Kriptografi modern beroperasi dalam bit atau byte, tidak seperti kriptografi klasik yang hanya beroperasi pada karakter. Salah satu algoritma kriptografi modern yang sedang berkemabng menjadi besar dan menjadi revolusi baru dalam sejarah kriptografi adalah kriptografi kunci-publik.

Kriptografi kunci-publik didesain untuk bertahan dari serangan *chosen-plaintext*, dan keamanan dari algoritma ini terletak pada kesulitan dalam mencari kunci rahasia dari kunci-publik. Pada saat ini, algoritma kriptografi kunci-publik yang paling biasa digunakan adalah algoritma RSA. Diperkirakan bahwa keamanan dari algoritma RSA terletak pada permasalahan faktor bilangan besar. Belum pernah ada pembuktian secara matematis bahwa diperlukan faktor dari modulus *n* untuk memecahkan suatu kriptogram dan kunci publik *{e, n}*. Dari sini dapat dipikirkan bahwa terdapat beberapa cara untuk memecahkan algoritma RSA (yang mungkin sudah dipecahkan oleh beberapa kriptanalis). Oleh karena itu dicarilah alternatif dai algoritma enkripsi kunci-publik seperti algoritma enkripsi ElGamal.

Seperti yang telah diketahui bahwa kemajuan dalam logaritma diskrit telah memaksa pengguna dari algorima kunci-publik ElGamal, bekerja dalam kumpulan nilai *GF(p)* yang berulang *(multiplicative group of GF(p))*, untuk meningkatkan bilangan prima modulus *p* agar mendapatkan tingkat keamanan yang diinginkan. Untuk keamanan jangka panjang, paling tidak terdapat 2000-bit modulo yang akan digunakan kemudian. Parameter yang digunakan bahkan membutuhkan ukuran kunci yang besar, karena menghitung basis data dari logaritma diskrit untuk satu keterangan *p* akan membuka rahasia dari seluruh kunci rahasia yang menggunakan *p*. Akan tetapi, untuk menemukan kumpulan nilai GF(p) yang berulang merupakan tugas yang tidak mudah dilakukan jika $p > 2^{2000} \approx 0.115 \times 10^{603}$.

1.2 Ruang Lingkup

Untuk tidak memperluas area pembahasan yang terdapat pada makalah, maka penulis memfokuskan permasalahan pada kumpulan nilai GF(p) yang berulang *(multiplicative group of GF(p))* yang akan dimodifikasi sehingga algoritma ElGamal dapat bekerja menggunakan kumpulan nilai GF(p^m) yang berulang, subgroup dari kumpulan nilai GF(p^m) dan sebuah sistem aljabar yang dinamakan kumpulan nilai palsu GF(p^m) yang berulang (spurious multiplicative group of GF(p^m)).

1.3 Tujuan Penulisan

Tujuan yang hendak dicapai dari penulisan makalah ini adalah untuk melakukan modifikasi penggunaan *multiplicative group* pada algoritma ElGamal dan juga melakukan analisis terhadap keamanannya. Hasil yang dicapai diharapkan dapat meningkatkan keamanan dalam pengiriman pesan sehingga dapat memberikan jaminan integritas data serta menjaga kerahasiaan.

2 DASAR TEORI

2.1 Kriptografi Kunci-publik

Sampai akhir tahun 1975, hanya ada kriptografi kunci-simetri. Karena kriptografi simetri menggunakan kunci yang sama untuk enkripsi dan dekripsi, maka hal ini mengimplikasikan dua pihak yang berkomunikasi saling mempercayai. Salah satu masalah di dalam sistem ini adalah cara mendistribusikan kunci. Kunci itu harus dikirim melalui saluran yang aman (kurir) atau bertemu secara langsung untuk membagi kunci. Perhatikan bahwa saluran kedua itu umumnya lambat dan mahal.

Masalah ini dipecahkan oleh Diffie dan Hellman dengan mengusulkan kriptografi asimetri yang memungkinkan pengguna berkomunikasi secara aman tanpa perlu berbagi kunci rahasia. Nama lainnya adalah kriptografi kunci-publik, sebab kunci untuk enkripsi diumumkan untuk publik, sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan. Siapapun dapat mengirim pesan yang dienkripsi dengan kunci publik tersebut, tetapi hanya penerima pesan yang dapat mendekripsi pesan menggunakan kunci rahasia miliknya sendiri.

Algoritma ElGamal merupakan algoritma enkripsi kunci asimetris untuk kriptografi kunci publik yang didasari kesepakatan kunci Diffie-Hellman. Pada tahun 1984, Taher ElGamal mempresentasikan suatu kriptosistem yang berdasarkan permasalahan logaritma diskrit [3]. Kriptosistem ini didasari oleh asumsi bahwa permasalahan logaritma diskrit tidak dapat ditemukan dengan mudah, sementara operasi *inverse* dapat dihitung secara efisien.

Kriptografi kunci-publik dapat dianalogikan seperti kotak surat yang terkunci dan memiliki lubang untuk memasukkan surat. Setiap orang dapat memasukkan surat ke dalam kotak tersebut, tetapi hanya pemilik kotak yang dapat membukakotak dan membaca surat di dalamnya karena ia yang memiliki kuncinya.

Keuntungan kriptografi kunci-publik ada dua. Pertama, kunci publik dapat dikirim ke penerima melalui saluran yang sama dengan saluran yang digunakan untuk mengirim pesan (saluran untuk mengirim pesan umunya tidak aman). Kedua, jumlah kunci dapat ditekan. Untuk berkomunikasi dengan banyak orang tidak perlu kunci rahasia sebanyak orang tersebut, cukup membuat dua kunci, yaitu kunci publik dan kunci rahasia.

2.2 Algoritma ElGamal

Algoritma ElGamal merupakan algoritma enkripsi kunci asimetris untuk kriptografi kunci publik yang didasari kesepakatan kunci Diffie-Hellman. Pada tahun 1984, Taher ElGamal mempresentasikan suatu kriptosistem yang berdasarkan permasalahan logaritma diskrit [3]. Kriptosistem ini didasari oleh asumsi bahwa permasalahan logaritma diskrit tidak dapat ditemukan dengan mudah, sementara operasi *inverse* dapat dihitung secara efisien.

Sistem kunci-publik orisinil yang diberikan oleh Diffie dan Hellman membutuhkan interaksi dari kedua belah pihak untuk menghitung kunci rahasia. Hal ini dapat menimbulkan masalah apabila kriptosistem ini diterapkan ke dalam suatu sistem komunikasi dimana kedua belah pihak tidak dapat berinteraksi karena adanya keterlambatan dalam transmisi atau karena pihak yang menerima sedang tidak ada.

Algoritma ElGamal menyederhanakan algoritma pertukaran kunci Diffie-Hellman dengan memperkenalkan bilangan eksponen acak k. Bilangan eksponen ini menggantikan bilangan eksponen rahasia dari pihak penerima. Hasil dari penyederhanaan algoritma ini dapat digunakan untuk melakukan enkripsi dalam satu arah, tanpa perlu mendapatkan interaksi dari pihak kedua.

Keunggulan dari kunci ini yaitu algoritma ini dapat digunakan untuk melakukan enkripsi pesan elektronik yang ditransmisi melalui layanan simpan dan teruskan (*store-and-forward services*).

3 PERANCANGAN MODIFIKASI ALGORITMA ELGAMAL

Seperti yang telah dijelaskan pada bab pertama, bahwa untuk menemukan kumpulan nilai GF(p) yang berulang merupakan tugas yang tidak mudah dilakukan jika $p > 2^{2000} \approx 0.115 \times 10^{603}$, akan tetapi adalah hal yang mungkin untuk mengatasi gangguan ini dengan menggunakan kriptosistem kunci-publik ElGamal yang bekerja dalam kumpulan nilai $GF(p^m)$ yang berulang *(multiplicative group of* $GF(p^m)$*)* dan bahwa bilangan primitif polinomial *p(x)* dari derajat *m* suatu *GF(p)* akan digunakan untuk membentuk $GF(p^m)$.

Karena akar dari bilangan primitif polinomial *p(x)* diketahui, maka dapat diketahui dengan mudah generator dari kumpulan nilai $GF(p^m)$ yang berulang, yaitu suatu elemen primitif dari *field* tersebut. Dan ternyata, *cipher* ini juga bekerja pada subgroup dari kumpulan nilai $GF(p^m)$ dan bahkan pada suatu sistem aljabar yang dinamakan kumpulan nilai palsu $GF(p^m)$ yang berulang (*spurious multiplicative group of* $GF(p^m)$) dan disingkat menjadi $SMG(p^m)$.

3.1 Implementasi skema Algoritma ElGamal dengan menggunakan kumpulan nilai GF(p^m) yang berulang (multiplicative group of GF(p^m))

Walau diketahui bahwa skema dasar enkripsi ElGamal dapat digeneralisasi untuk bekerja dalam semua kumpulan bilangan terbatas yang berulang, terutama dalam kumpulan nilai $GF(p^m)$ yang berulang, dan bahwa operasi terhadap elemen dari kumpulan nilai $GF(p^m)$ yang berulang, yaitu perkalian dan eksponensial, sangat mudah untuk diimplementasikan dan permasalahan logaritma diskrit pada kumpulan ini akan menjadi tidak mudah untuk dipecahkan [4], tidak dibutuhkan pendekatan praktik yang serius untuk mengimplementasikan sistem ini.

Deskripsi ringkas mengenai modifikasi algoritma yang dilakukan, akan dijelaskan di bawah ini.

Pembangkit kunci: Setiap entitas menghasilkan kunci-publik dan kunci-rahasia yang saling berkoresponden. Sehingga setiap entitas A dapat melakukan:

- Memilih bilangan primitif polinomial $p(x)$ dari dari derajat m suatu $GF(p)$ untuk membentuk kumpulan nilai $GF(p^m)$ yang berulang. Kumpulan ini mempunyai urutan $n= p^m-1$, terdiri dari set $G = \{1,...,p^m-1\}$ dan operasi perkalian dan eksponensial suatu elemen dari set ini yang ditunjukan oleh persamaan $P(x,y), x,y \in G$. Fungsi $Pow(x,k)$ membawa operasi seluruh elemen yang muncul dari G sampai a k-th, $k \in [-n+1,n-1]$, juga didefinisikan. Generator dari kupulan ini adalah p, semenjak polinomial $p(x)$ merupakan bilangan primitif.
- Memilih bilangan integer acak $r \in [1, n-2]$ seperti $(r, n-1) =1$, dan menghitung generator lain $\alpha = Pow(p,r)$.
- Memilih bilangan integer acak $a \in G$, dan menghitung $\beta = Pow(\alpha,a)$.
- Kunci-publik A adalah α dan β, bersama $p(x)$ dan fungsi P dan Pow, apabila ketiga parameter terakhir tidak cocok dengan semua entitas.
- Kunci-rahasia A adalah a.

Enkripsi: Entitas B melakukan enkripsi terhadap pesan m yang akan dikirim kepada A. Maka B melakukan langkah sebagai berikut:

- Mendapatkan kunci-publik A yaitu α,β dan $p(x)$ bersama fungsi P dan Pow apabila parameter tersebut tidak cocok.
- Merepresentasikan pesan m sebagai kumpulan nilai G.
- Memilih bilangan integer acak $k \in [1, n-1]$.
- Menentukan nilai $c_1 = Pow(\alpha,k)$ dan $c_2 = P(m,Pow(\beta,k))$.
- Mengirim cipherteks $c=c_1, c_2$ kepada A.

Dekripsi: Untuk mendapatkan plainteks m dari cipherteks $c=c_1, c_2$, entitas A harus melakukan langkah sebagai berikut:

- Menggunakan kunci-rahasia a untuk menghitung $g = Pow(c_1,a)$ dan kemudian menghitung $g^{-1} = Pow(g,-1)$.
- Mendapatkan plainteks dengan menghitung $m = P(g^{-1}, c_2)$.

3.2 Modifikasi implementasi skema Algoritma ElGamal dengan menggunakan kumpulan nilai GF(p^m) yang berulang, subgroup dari kumpulan nilai GF(p^m) dan sebuah sistem aljabar yang dinamakan kumpulan nilai palsu GF(p^m) yang berulang (spurious multiplicative group of GF(p^m))

Jika diasumsikan bahwa untuk membentuk kumpulan nilai $GF(p^m)$ yang berulang akan digunakan bilangan primitif polinomial, tetapi untuk menentukan bilangan primitif polinomial dari derajat yang lebih tinggi tidaklah mudah. Terdapat beberapa tabel yang berguna [6], diman terdapat sekitar 600 bilangan primitif polinomial dari derajat 311 sampai 3604 dari $GF(2)$ yang terdaftar. Sangat disayangkan bahwa sangat sulit untuk mencari tabel yang mirip untuk bilangan ganjil p. Meskipun demikian, dengan menggunakan sistem komputer aljabar memudahkan untuk menentukan bilangan polinomial acak yang tidak dapat diperkecil lagi dalam derajat m dari $GF(p)$, dengan bilangan ganjil p yang memenuhi $p^m \in [2^{1000},2^{5000}]$ dan bekerja menggunakan skema enkripsi ElGamal berdasarkan subgroup dari kumpulan nilai $GF(p^m)$ yang berulang dengan besar kunci antara 1000-5000 bit.

Deskripsi yang lebih detil dari implementasi skema enkripsi ElGamal menggunakan kumpulan nilai $GF(p^m)$ yang berulang, subgroup dari kumpulan nilai $GF(p^m)$ dan juga kumpulan nilai palsu $GF(p^m)$ yang berulang ($SMG(p^m)$) diberikan dalam (Koscielny, 2003) [6]. Dari ketiga kasus ini, dapat digunakan rutinitas P dan Pow yang sama, dan juga bilangan primitif polinomial, bilangan polinomial yang tidak dapat diperkecil lagi, dan bilangan polinomial dari $GF(p)$ secara berturut-turut. Karena notasi dari kumpulan nilai palsu $GF(p^m)$ yang berulang merupakan hal yang baru, maka sistem aljabar ini akan dijelaskan pada subBab berikutnya.

3.3 Kumpulan nilai palsu $GF(p^m)$ yang berulang ($SMG(p^m)$)

Untuk setiap bilangan prima p, dan setiap bilangan integer positif m dan polinomial $f(x)$ derajat m dari $GF(p)$ terdapat suatu sistem aljabar $<Gx, \cdot>$, terdiri dari set Gx dari semua p^m-1 polinomial bukan nol derajat $dg \leq m-1$ dari $GF(p)$ dan dari operasi perkalian polinomial modulo polinomial $f(x)$. Sistem aljabar ini merupakan generalisasi dari kumpulan nilai $GF(p^m)$ yang berulang, karena elemen dari set Gx merupakan elemen yang sama dari kumpulan nilai

$GF(p^m)$ yang berulang. Oleh karena itu, sistem ini disebut kumpulan nilai palsu $GF(p^m)$ yang berulang (*spurious multiplicative group of* $GF(p^m)$) dan disingkat menjadi $SMG(p^m)$. $SMG(p^m)$ didapat dari pemetaan σ, didefinisikan melalui fungsi $\sigma(v(x))=v(p)$, mengubah polinomial $v(x)$ yang dimilik set Gx menjadi suatu bilangan dari set G. Perkalian di dalam $SMG(p^m)$ dapat langkah yang sama atau dengan perangkat keras yang sama yang digunakan dalam perkalian $GF(p^m)$, tetapi bagian dalam dari tabel $SMG(p^m)$ bukanlah huruf latin.

Dibawah ini dapat dilihat contoh tabel operasi $SMG(2^3)$, yang dibentuk menggunakan polinomial $x^3+1 = (x+1)(x^2+x+1)$ pada Tabel 1. Sebagai contoh, kalikan x dengan $x^2 \pmod{x^3+1}$. Hasilnya adalah 1. Tapi semenjak dalam kasus dipertimbangkan bahwa $p=2$, maka akan didapat $\sigma(x)=2$ *dan* $\sigma(x^2)=4$, maka $2 \cdot 4=4 \cdot 2=1$. Hal yang serupa juga dapat dilihat pada berikut ini, $(x+1) \cdot (x^2+x+1)=x^3+1 \equiv 0 \pmod{x^3+1}$, dan sehingga $7 \cdot 3=3 \cdot 7=0$.

.	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	1	3	5	7
3	3	6	5	5	6	3	0
4	4	1	5	2	6	3	7
5	5	3	6	6	3	5	0
6	6	5	3	3	5	6	0
7	7	7	0	7	0	0	7

Tabel 1. Tabel operasi $SMG(2^3)$ yang dibentuk menggunakan $f(x)=x^3+1$ dan pemetan σ.

4 ANALISIS

Untuk modifikasi implementasi skema Algoritma ElGamal dengan menggunakan kumpulan nilai $GF(p^m)$ yang berulang dan subgroup dari kumpulan nilai $GF(p^m)$, dari subBab pertama Bab ketiga, dapat dilihat bahwa algoritma enkripsi yang dihasilkan mudah untuk diggunakan, karena pada skema tersebut, algoritma pembangkit kunci, enkripsi dan dekripsi sangat sederhana dan efektif, meskipun besar kunci yang dibutuhkan mencapai 10000 bit atau lebih.

Sedangkan untuk modifikasi implementasi skema Algoritma ElGamal dengan menggunakan kumpulan nilai palsu $GF(p^m)$ yang berulang ($SMG(p^m)$), berdasarkan prinsip, $SMG(p^m)$ merupakan kumpulan komutatif, sehingga operasi dapat bersifat tertutup ataupun tidak sepenuhnya asosiatif, karena pembagi 0 hanya ada jika $f(x)$ tidak dapat diperkecil lagi.

Keberadaan dari penggunaan kelompok $SMG(p^m)$ masih tergolong sangat baru. Oleh karena itu semua propertinya belum dianalisis lebih lanjut. Namun begitu menggunakan skema enkripsi ElGamal berdasarkan $SMG(p^m)$, kita harus ingat bahwa ada elemen tidak-nol yang tergabung dalam kelompok ini yang tidak memiliki invers multiplikatif. Himpunan dari semua elemen reversibel membentuk sebuah kelompok Abelian dibawah perkalian (fungsi P), yang secara umum tidak siklik. Kemudian dapat dilihat bahwa pesan apapun dapat dienkripsi oleh rata-rata dari skema enkripsi ElGamal berdasarkan $SMG(p^m)$, kecuali pengirim, setelah kriptogram $c=c_1,c_2$ telah dibangkitkan, maka harus memverifikasi jika c_1 dapat dibalik kembali, yaitu jika $Pow(c_1,-1)$ ada dan dapat dikomputasi. Hal ini merupakan kondisi yang penting untuk sebuah kesuksesan ciphering.

5 KESIMPULAN

Dari hasil analisis terhadap modifikasi kumpulan nilai (*multiplicative group*) yang terdapat pada skema algoritma ElGamal , penulis dapat mengambil kesimpulan, yaitu:

1. Telah ditunjukan bahwa algoritma enkripsi kunci-publik ElGamal berdasarkan kumpulan nilai $GF(p^m)$ yang berulang, subgroup dari kumpulan nilai $GF(p^m)$ mudah untuk digunakan.
2. Hal yang paling menarik disini adalah penggunaan nilai palsu $GF(p^m)$ yang berulang ($SMG(p^m)$), yang menjadikan kriptosistem lebih tidak dapat diperkirakan dan menambah besar kunci. Dengan kata lain, misalkan $SMG(S^{20000})$ digunakan, maka dapat dibentuk $2^{20000} \approx 0.398x10^{6021}$ nilai palsu yang berulang dan kunci kriptosistem ElGamal sebesar 20000 bit dapat bekerja. Akan tetapi, masalah ini masih tergolong sangat baru dan masih belum didiskusikan lebih mendalam.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, 2006.

[2] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2008.

[3] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proceedings* of CRYPTO 84 *on Advances in cryptology*, pages 10–18. Springer-Verlag New York, Inc., 1985.

[4] Stinson D.R., *Cryptography Theory and Practice*. BocaRaton: CRC Press,1995

[5] Živkovic´ M.(1994), Table of primitive binary polynomials, PartII. —Math. Comput., Vol.63, No. 207, pp.301–306.

[6] http://www.mapleapps.com/List.asp?CategoryID=6& Category=Cryptography

[7] http://en.wikipedia.org/wiki/Elgamal