Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa

[1]Anandia Zelvina, [1]Syahril Efendi, [1]Dedy Arisandi

[1]Program Studi S1 Teknologi Informasi
Fakultas Ilmu Komputer dan Teknologi Informasi
Universitas Sumatera Utara
E-mail: anandiazelvina@gmail.com, syahril1@usu.ac.id, dedyarisandi@gmail.com

***Abstrak*— Dalam perkuliahan komputer, kriptografi menjadi salah satu mata kuliah yang diajarkan. Pembelajaran kriptografi menjadi sangat penting bagi mahasiswa komputer agar mengetahui cara-cara mengamankan data. Pada penulisan artikel ilmiah ini akan dijelaskan cara-cara mengamankan data menggunakan algoritma ElGamal. Algoritma ElGamal dalam pembentukan salah satu kuncinya menggunakan bilangan prima dan menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit. Sehingga, dengan menggunakan bilangan prima yang besar serta masalah logaritma diskrit yang cukup menyulitkan maka keamanan kuncinya akan lebih terjamin. Dari penelitian ini akan dihasilkan aplikasi pembelajaran kriptografi kunci publik ElGamal yang dapat memudahkan mahasiswa untuk mempelajari kriptografi.**

***Kata Kunci*—Kriptografi, Mengamankan Data, Algoritma ElGamal, Bilangan Prima, Logaritma Diskrit**

I. PENDAHULUAN

Dalam kehidupan sehari-hari manusia banyak bergantung pada teknologi informasi, baik dari hal kecil hingga ke permasalahan yang rumit. Contoh teknologi informasi dalam kehidupan sehari-hari yaitu *ATM, Internet Banking, Mobile Banking, Email, SMS, MMS, Chatting* dan sebagainya [1]. Kemajuan teknologi informasi memberikan banyak keuntungan bagi kehidupan manusia. Tetapi keuntungan yang ditawarkan oleh teknologi informasi juga menimbulkan kejahatan seperti pencurian data. Sehingga perkembangan ilmu untuk mengamankan data semakin ditingkatkan agar pengguna teknologi selalu merasa aman. Berbagai cara dilakukan untuk menjaga keamanan data tersebut. Salah satunya dengan menyandikan data menjadi suatu kode-kode yang tidak dimengerti, sehingga apabila disadap akan kesulitan untuk mengetahui informasi yang sebenarnya.

Metode penyandian yang pertama kali dibuat masih menggunakan metode algoritma rahasia. Metode ini menumpukan pada kerahasiaan algoritma yang digunakan. Namun metode ini tidak efisien saat harus digunakan untuk berkomunikasi dengan banyak orang. Oleh karena itu, seseorang harus membuat algoritma baru apabila akan bertukar informasi rahasia dengan orang lain. Karena penggunanya merasa tidak efisien maka algoritma rahasia mulai ditinggalkan dan dikenalkan suatu metode baru yang disebut dengan algoritma kunci. Metode ini tidak menumpukan keamanan pada algoritmanya, tetapi pada kerahasiaan kunci yang digunakan pada proses peyandiannya. Algoritmanya dapat diketahui dan dipelajari oleh siapapun. Metode algoritma kunci mempunyai tingkat efisiensi dan keamanan yang lebih baik dibandingkan dengan algoritma rahasia. Algoritma kunci yang dikenal dengan kriptografi telah melingkupi aspek kehidupan manusia saat ini. Begitu pentingnya kriptografi, saat berbicara tentang keamanan komputer orang tidak bisa memisahkannya dengan kriptografi [2].

Pada perkuliahan komputer, kriptografi menjadi salah satu mata kuliah yang diajarkan. Pembelajaran kriptografi menjadi sangat penting bagi mahasiswa komputer agar mengetahui cara-cara mengamankan data. Oleh karena itu penulis akan membuat aplikasi pembelajaran bagi mahasiswa khususnya pembelajaran kriptografi kunci publik ElGamal.

Algoritma ElGamal merupakan salah satu dari algoritma kunci. Algoritma ini dikembangkan pertama kali oleh Taher ElGamal pada tahun 1985. Sampai saat ini, algoritma ElGamal masih dipercaya sebagai metode penyandian, seperti aplikasi PGP dan GnuPG yang dapat digunakan untuk pengamanan e-mail dan tanda tangan digital. Pada tahun 1994 pemerintah Amerika Serikat mengadopsi *Digital Signature Standard*, sebuah mekanisme penyandian yang berdasar pada algoritma ElGamal [3].

II. IDENTIFIKASI MASALAH

Kriptografi sangat penting untuk dipelajari. Saat ini pembelajaran pun mulai dikemas secara lebih praktis dan menarik melalui media komputer karena komputer mampu menampilkan teks, warna, suara, video, gerak, gambar serta mampu menampilkan kepintaran yang dapat menyajikan proses interaktif. Media komputer dimanfaatkan dalam pembelajaran karena memberikan keuntungan-keuntungan yang tidak dimiliki oleh media pembelajaran lainnya yaitu kemampuan komputer untuk berinteraksi secara individu

dengan mahasiswa. Model pembelajaran yang diterapkan dalam pembelajaran berbantuan komputer secara umum dapat diklasifikasikan menjadi empat model, yaitu *tutorial, drill and practice*, *simulation* dan *problem-solving.* Dalam model *tutorial* dan *drill and practice*, komputer berperan sebagai pengajar, sedangkan model *simulation* dan *problem-solving*, untuk mengembangkan penggunaan kemampuan memecahkan masalah melalui p endekatan *discovery* atau *exploratory*. Beberapa hasil penelitian menyatakan bahwa pembelajaran ini dapat meningkatkan motifasi belajar, media pembelajaran yang efektif, tidak adanya batas ruang dan waktu belajar [4].

Kriptografi adalah salah satu mata kuliah yang diajarkan di bidang ilmu komputer. Kriptografi harus ajarkan agar mahasiswa mengetahui cara-cara mengamankan data. Untuk mengatasi hal tersebut, diperlukan pembelajaran tentang pengamanan data yaitu menggunakan metode kriptografi kunci publik ElGamal. Oleh karena itu ilmu untuk mengamankan data harus semakin ditingkatkan. Untuk mengatasi hal tersebut, diperlukan pembelajaran tentang pengamanan data yaitu menggunakan metode kriptografi kunci publik ElGamal.

Pada artikel ilmiah ini penulis membuat aplikasi pembelajaran kriptografi kunci publik ElGamal untuk mahasiswa menggunakan bahasa pemrograman Microsoft Visual Studio 2008. Pembuatan aplikasi ini juga ditujukan agar mahasiswa dapat mengetahui proses ekripsi dan dekripsi menggunakan algoritma ElGamal serta dapat menentukan private key dan public key algoritma ElGamal.

III. PENELITIAN TERDAHULU

Ada beberapa penelitian yang telah dilakukan pada algoritma ElGamal. Salah satunya adalah Metode Enkripsi dan Dekripsi dengan menggunakan Algoritma ElGamal. Pada penelitian ini diperoleh bahwa algoritma ElGamal keamanannya terletak pada logaritma diskrit pada grup pergandaan bilangan bulat modulo prima, dengan mengambil nilai bilangan prima yang besar, maka upaya pemecahan pesan akan sangat sukar [5].

Adapun penelitian lainnya yan berkaitan dengan algoritma ElGamal adalah Aplikasi Pengamanan Dokumen Office Dengan Algoritma Kriptografi Kunci Asimetris ElGamal. Dalam penelitian ini disimpulkan bahwa Implementasi program ini menghasilkan suatu aplikasi yang mengubah isi dokumen (plaintext) yang berupa text, table dan gambar menjadi kode-kode yang tidak dikenal (ciphertext) [6].

IV. METODE PENELITIAN

A. *Kriptografi*

Kriptografi berasal dari bahasa Yunani, “kryptós” yang berarti tersembunyi dan “gráphein” yang berarti tulisan. Sehingga kata kriptografi dapat diartikan menjadi “tulisan tersembunyi”. Menurut Request for Comments (RFC), kriptografi adalah ilmu matematika yang berhubungan dengan transformasi data agar arti dari data tersebut menjadi sulit untuk dipahami (untuk menyembunyikan maknanya), mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaan yang tidak sah. Jika transformasinya dapat dikembalikan, kriptografi juga dapat diartikan sebagai proses mengubah kembali data yang terenkripsi menjadi bentuk yang mudah dipahami. Sehingga, kriptografi juga dapat diartikan sebagai proses untuk melindungi data dalam arti yang luas [7].

Pengertian Kriptografi dalam kamus bahasa Inggris Oxford adalah sebagai berikut :

“ Sebuah teknik rahasia dalam penulisan, dengan karakter khusus, dengan mengguanakan huruf dan karakter di luar bentuk aslinya, atau dengan metode-metode lain yang hanya dapat dipahami oleh pihak-pihak yang memproses kunci, juga semua hal yang ditulis dengan cara seperti ini.”

Jadi, secara umun kriptografi diartikan sebagai seni menulis atau memecahkan cipher [8].

Kriptografi mempunyai sejarah yang panjang dan menakjubkan. Informasi yang lengkap mengenai sejarah kriptografi dapat dilihat pada buku David Kahn yang berjudul *The Codebreakers*. Buku dengan tebal 1000 halaman ini menuliskan secara jelas tentang sejarah kriptografi mulai dari penggunaan kriptografi oleh Bangsa Mesir 4000 tahun yang lalu (berupa *hieroglyph* yang terdapat pada piramid) hingga penggunaan kriptografi pada abad ke-20 [9].

B. *Jenis Algoritma Kriptografi*

Berdasarkan jenis kunci, algoritma kriptografi dikelompokan menjadi dua bagian, yaitu : algoritma simetris (algoritma kunci privat) dan algoritma asimetris (algoritma kunci publik) [9].

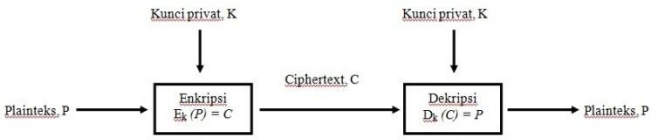
Algoritma Simetris

Algoritma simetris adalah salah satu jrnis kunci pada algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Istilah lain untuk kriptografi kunci simetri adalah kriptografi kunci privat (*private-key cryptography*). Sistem kriptografi kunci-simetri diasumsikan sebagai pengirim dan penerima pesan yang sudah berbagi kunci yang sama sebelum bertukar pesan. Keamanan sistem kriptografi simetri terletak pada kerahasiaan kuncinya.

Kriptografi simetri adalah jenis kriptografi yang diketahui masuk ke dalam catatan sejarah hingga tahun 1976. Semua algoritma kriptografi klasik termasuk ke dalam sistem kriptografi simetri. Salah satu kelebihan pada algoritma simetris yaitu proses enkripsi dan deskripsinya jauh lebih cepat dibandingkan dengan algoritma asimetris. Sedangkan kelemahannya yaitu pada permasalahan distribusi kunci (*key distribution*).

Seperti yang telah dibahas sebelumnya, proses enkripsi dan deskripsi pada kriptografi simetri menggunakan kunci yang sama. Sehingga timbul persoalan untuk menjaga kerahasian kunci. Contohnya pada saat pengiriman kunci dilakukan melalui media yang tidak aman seperti internet. Jika kunci ini hilang atau sudah diketahui oleh orang yang

tidak berhak, maka kriptosistem ini dinyatakan tidak aman lagi. Kelemahan lain adalah masalah efisiensi jumlah kunci. Jika terdapat *n* user, maka diperlukan *n*(*n*-1)/2 kunci, sehingga untuk jumlah user yang sangat banyak, sistem ini tidak efisien lagi [9].



Gambar 1. Skema Kriptografi Simetri

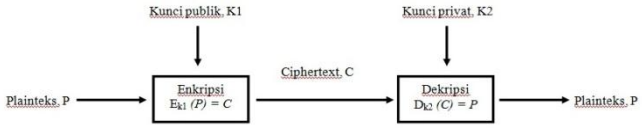
Algoritma Asimetris

Algoritma asimetris atau dapat disebut juga dengan algoritma kunci public, didesain sebaik mungkin sehingga kunci yang digunakan untuk enkripsi berbeda dengan kunci dekripsinya. Dimana kunci untuk enkripsi tidak rahasia (diumumkan ke publik), sementara kunci dekripsinya bersifat rahasia (hanya diketahui oleh penerima pesan).

Pada kriptografi asimetris, setiap orang yang akan berkomunikasi harus mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Pengirim pesan akan mengenkripsi pesan menggunakan kunci publik si penerima pesan dan hanya penerima pesan yang dapat mendekripsi pesan tersebut karena hanya ia yang mengetahui kunci privatnya sendiri. Kriptografi kunci-publik dapat dianalogikan seperti kotak surat yang terkunci dan memiliki lubang untuk memasukkan surat. Setiap orang dapat memasukkan surat ke dalam kotak surat tersebut, tetapi hanya pemilik kotak yang dapat membuka kotak dan membaca surat di dalamnya karena ia yang memiliki kunci. Sistem ini memiliki dua keuntungan. Yang pertama yaitu, tidak ada kebutuhan untuk mendistribusikan kunci privat sebagaimana pada sistem kriptografi simetri. Kunci publik dapat dikirim ke penerima pesan melalui saluran yang sama dengan saluran yang digunakan untuk mengirim pesan. Saluran untuk mengirim pesan umumnya tidak aman.

Kedua, jumlah kunci yang digunakan untuk berkomunikasi secara rahasia dengan banyak orang tidak perlu sebanyak jumlah orang tersebut, cukup membuat dua buah kunci, yaitu kunci publik bagi para koresponden untuk mengenkripsi pesan, dan kunci privat untuk mendekripsi pesan. Berbeda dengan kriptografi kunci-simetris yang membuat kunci sebanyak jumlah pihak yang diajak berkorespondensi.

Meski masih terbilang baru (sejak 1976), kriptografi kunci-publik mempunyai kontribusi yang luar biasa dibandingkan dengan sistem kriptografi simetri. Kontribusi yang paling penting adalah tanda-tangan digital pada pesan untuk memberikan aspek keamanan otentikasi, integritas data, dan nirpenyangkalan. Tanda-tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci yang digunakan. Pengirim pesan mengenkripsi pesan (yang sudah diringkas) dengan kunci privatnya, hasil enkripsi inilah yang dinamakan tanda-tangan digital. Tanda-tangan digital dilekatkan (embed) pada pesan asli. Penerima pesan memverifikasi tanda-tangan digital dengan menggunaklan kunci publik.



Gambar 2. Skema Kriptografi Asimetri

C. Tujuan Kriptografi

Tujuan dari kriptografi yang juga merupakan aspek keamanan informasi adalah sebagai berikut [9] :

1) Kerahasiaan (*confidentiality*) adalah layanan yang digunakan untuk menjaga isi informasi dari semua pihak kecuali pihak yang memiliki otoritas terhadap informasi. Ada beberapa pendekatan untuk menjaga kerahasiaan, dari pengamanan secara fisik hingga penggunaan algoritma matematika yang membuat data tidak dapat dipahami. Istilah lain yang senada dengan confidentiality adalah secrecy dan privacy.
2) Integritas data adalah layanan penjagaan pengubahan data dari pihak yang tidak berwenang. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam pesan yang sebenarnya. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (digital signature). Pesan yang telah ditandatangani menyiratkan bahwa pesan yang dikirim adalah asli.
3) Otentikasi adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (user authentication atau entity authentication) maupun mengidentifikasi kebenaran sumber pesan (data origin authentication). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diotentikasi asalnya. Otentikasi sumber pesan secara implisit juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. Oleh karena itu, layanan integritas data selalu dikombinasikan dengan layanan otentikasi sumber pesan. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (*digital signature*). Tanda-tangan digital menyatakan sumber pesan.
4) Nirpenyangkalan (*non-repudiation*) adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

D. Algoritma dan Kunci

Algoritma menggambarkan sebuah prosedur komputasi yang terdiri dari variabel input dan menghasilkan output

yang berhubungan [7]. Algoritma kriptografi adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi [10]. Algoritma kriptografi ini bekerja dalam kombinasi dengan menggunakan kunci (key) seperti kata, nomor atau frase tertentu.

Bila keamanan algoritma bergantung pada kerahasian algoritma yang bekerja, maka algoritma tersebut dikatakan sebagai algoritma yang memiliki kemampuan terbatas. Algoritma terbatas biasanya digunakan oleh sekelompok orang untuk bertukar pesan satu sama lain. Mereka membuat suatu algoritma enkripsi dan algoritma enkripsi tersebut hanya diketahui oleh anggota kelompok itu saja. Tetapi, algoritma terbatas tidak cocok lagi jika digunakaan saat ini, disebabkan karena setiap kali ada anggota kelompok yang keluar, maka algoritma kriptografi harus diganti lagi. Kerahasian algoritmanya menjadi suatu kelemahan karena tidak mengijinkan adanya kontrol kualitas atau standarisasi.

Kriptografi modern mengatasi masalah di atas dengan penggunaan kunci, dimana algoritma yang diguakan tidak lagi dirahasiakan, tetapi kunci harus dijaga kerahasiaannya. Kunci adalah parameter yang digunakan untuk transformasi *enciphering* dan *dechipering.* Kunci biasanya berupa *string* atau deretan bilangan. Dengan menggunakan kunci *K*, maka fungsi enkripsi dan dekripsi dapat ditulis sebagai

$$E_K(P) = C \; dan \; D_K(C) = P \quad (1)$$

dan kedua fungsi ini memenuhi

$$D_K(E_K(P)) = P \quad (2)$$

E. ElGamal

Algoritma ElGamal diciptakan oleh Taher ElGamal pada tahun 1984. Algoritma ini pada mulanya digunakan untuk kepentingan *digital signature*, namun kemudian dimodifikasi sehingga algoritma ElGamal bisa digunakan untuk enkripsi dan dekripsi. ElGamal digunakan di dalam perangkat lunak sekuriti yang dikembangkan oleh GNU, program PGP dan pada sistem sekuriti lainnya. Keamanan algoritma ini terletak pada sulitnya menghitung logaritma diskrit [2].

Logaritma ini disebut logaritma diskret karena nilainya berhingga dan bergantung pada bilangan prima yang digunakan. Karena bilangan prima yang digunakan adalah bilangan prima besar, maka sangat sulit bahkan tidak mungkin menurunkan kunci privat dari kunci publik yang diketahui walaupun serangan dilakukan dengan menggunakan sumberdaya komputer yang sangat besar.

F. Kelebihan Algoritma ElGamal

Algoritma ElGamal dikenal sebagai kriptografi *digital signature* karena algoritma ini berfungsi dengan baik untuk mengirimkan sebuah tanda tangan digital pada sebuah pesan. Kelebihan dari algoritma ElGamal yaitu:

1) Plainteks yang sama dapat diubah menjadi chiperteks yang berbeda, karena bilangan bulat pada algoritma Elgamal dapat dipilih secara acak untuk menentukan kunci.
2) Pada algoritma ElGamal tidak hanya kunci privat yang perlu dijamin kerahasiannya, tetapi autentikasi kunci publik juga harus tetap dijaga.
3) Kunci publik dan kunci privat pada algoritma ElGamal tidak perlu diubah dalam periode waktu yang panjang.
4) Algoritma ElGamal bisa dimanfaatkan untuk mengirimkan sebuah pesan rahasia, yaitu dengan menentukan kunci dari sebuah kriptografi simetris.

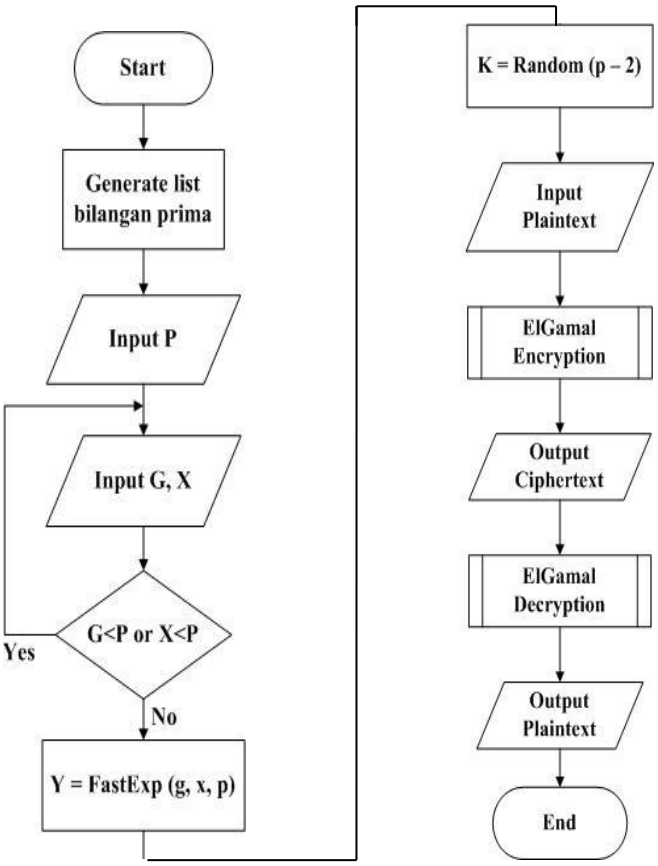
V. HASIL DAN PEMBAHASAN

A. Perancangan Flowchart

Untuk mempermudah proses perancangan sistem untuk implementasi algoritma ElGamal, perlu didefinisikan langkah-langkah yang dibuat kedalam *flowchart*.

Flowchart Sistem

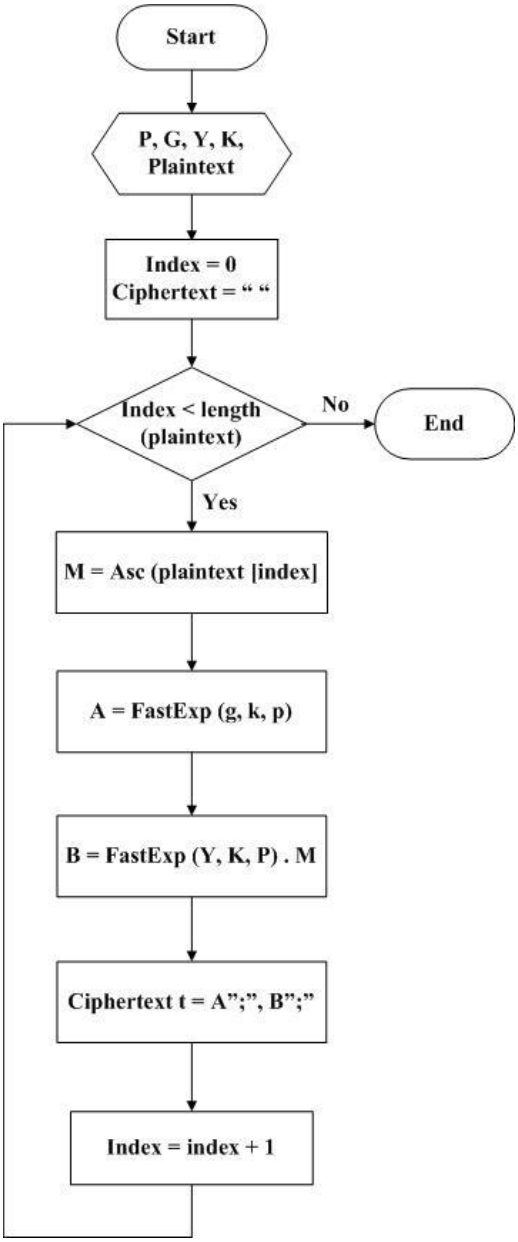
Flowchart sistem dibuat untuk menggambarkan bagaimana proses alur keseluruhan sistem bekerja.



Gambar 3. *Flowchart* Sistem

Flowchart ElGamal Encryption

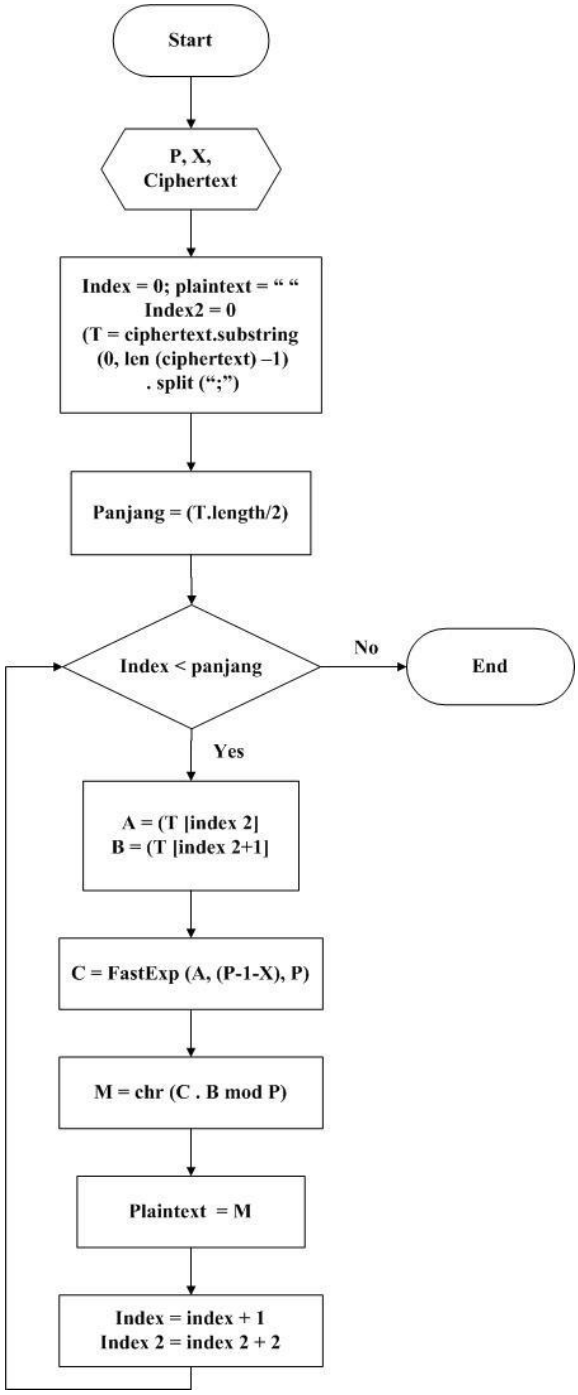
Flowchart ElGamal *encryption* dibuat untuk menggambarkan proses terbentuknya enkripsi.



Gambar 4. *Flowchart* ElGamal *Encryption*

Flowchart ElGamal Decryption

Flowchart pada ini hampir sama dengan *flowchart* pada proses enkrpsi.



Gambar 5. *Flowchart* ElGamal *Decryption*

B. Menu Teori

Pada menu teori ini berisi pembelajaran tentang algoritma-algoritma apa saja yang dipakai dalam sistem El Gamal ini. Terdapat dua algoritma yang dipakai yaitu Fast Exponensial dan ElGamal.

C. Menu Proses

Setelah menu teori pembelajaran Algoritma selanjutnya masuk ke dalam menu proses. Di dalam menu proses ini terdapat 4 pilihan yang dapat dipilih yaitu:

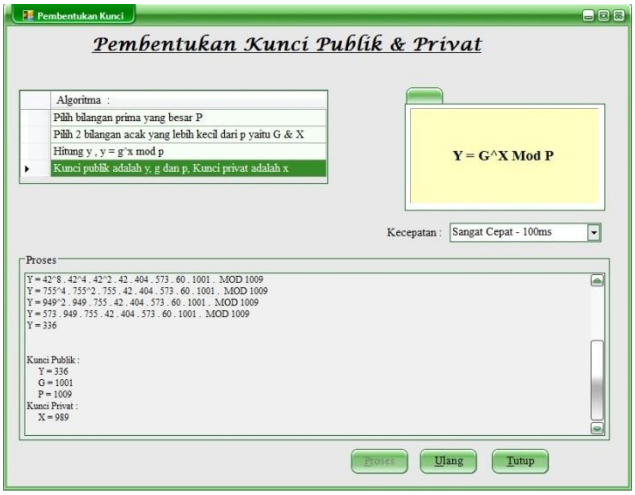
Cari Bilangan Prima

Pada tampilan ini terdapat tombol cari untuk menentukan bilangan prima dan tombol ini dapat digunakan setelah pengguna memasukkan angka pada kotak textbox. Tersedia juga tombol reset jika pengguna ingin tampilan ini kembali seperti tampilan awal. Pada proses ini dilakukan pencarian bilangan prima. Karena pada sistem ini diperlukan bilangan prima yang besar, sehingga harus dilakukan pencarian bilangan prima terlebih dahulu.

Gambar 6. Cari Bilangan Prima

Pembentukan Kunci

Pada tampilan ini diberikan langkah-langkah pembentukan kunci pada kotak algoritma, lalu pada kotak TabControl pengguna dapat memasukkan bilangan prima besar. Tampilan ini diberikan fasilitas kecepatan proses pembentukan kunci dan kotak proses yang menampilkan proses pembentukan kunci. Terdapat juga tombol ulang juka pengguna ingin kembali mencoba ulang proses pembentukan kunci serta tombol tutup agar pengguna dapat keluar dari tampilan ini. Pada proses ini akan diperoleh kunci publik adalah y, g dan p, kunci privat adalah x.



Gambar 7. Pembentukan kunci publik & privat

Enkripsi ElGamal

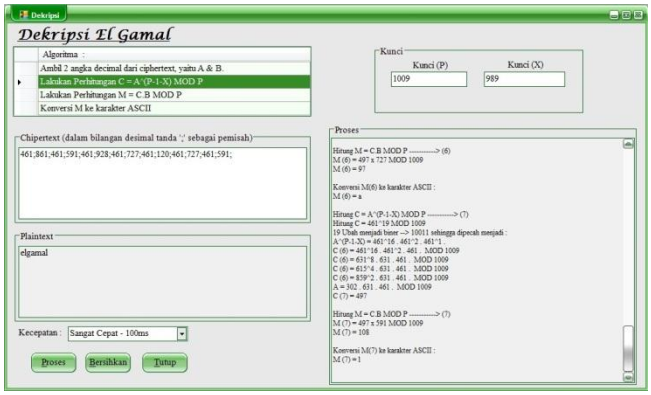
Sama seperti rancangan pada proses pembentukan kunci yang diberikan kotak algoritma agar pengguna mengetahui langkah-langkah proses enkripsi. Lalu pada kotak kunci terdapar kunci P, G, dan Y yang telah ditentukan sebelumnya, serta kunci K yang dapat diacak langsung menggunakan tombol acak. Pada kotak plainteks, pengguna dapat memasukkan kalimat yang diinginkan dan hasil cipherteksnya akan keluar pada kotak cipherteks setelah dilakukannya proses pada kotak proses. Terdapat juga fasilitas kecepatan yang dapat ditentukan oleh pengguna, serta tombol bersihkan untuk membersihkan tampilan ini dan tombol tutup untuk keluar dari tampilan.Setelah pembentukan kunci, proses selanjutnya yang dilakukan yaitu proses enkripsi dan diperoleh pasangan A dan B yang merupakan Ciphertext.

Gambar 8. Enkripsi ElGamal

Dekripsi ElGamal

Rancangan ini hampir sama seperti rancangan pada proses enkripsi. Yang membedakannya adalah pada kotak kunci. Jika pada proses enkripsi terdapat kunci P, G, Y dan K, maka pada proses dekripsi hanya terdapat kunci P dan X saja. Lain halnya dengan proses enkripsi yang kotak cipherteksnya diletakkan dibawah kotak plainteks. Pada rancangan proses

dekripsi ini kotak cipherteks diletakkan diatas kotak plainteks, karena pada tampilan ini cipherteks telah ditentukan sebelumnya melalui proses enkripsi. Fasilitas yang disediakan pada rancangan tampilan ini juga masih sama dengan rancangan tampilan proses enkripsi. Setelah proses Enkripsi El Gamal dilakukan selanjutnya masuk ke dalam tahap proses dekripsi El Gamal. Pada tahap ini diperoleh plaintext yang telah ditentukan pada proses enkripsi.



Gambar 9. Dekripsi ElGamal

I. KESIMPULAN DAN SARAN

Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Plainteks yang akan dienkripsi dipecah menjadi blok-blok plainteks, selanjutnya proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi dan hasilnya digabungkan kembali menjadi pesan yang utuh dan dapat dimengerti. Kriptografi kunci publik ElGamal dapat digunakan untuk mengamankan data karena algoritma ElGamal dalam pembentukan salah satu kuncinya menggunakan bilangan prima dan menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit sehingga keamanan kuncinya lebih terjamin.

Dengan adanya aplikasi ini, mahasiswa dapat mengetahui proses enkripsi dan dekripsi pada algoritma ElGamal. Algoritma ElGamal juga bisa dimanfaatkan untuk mengirimkan sebuah pesan rahasia yang sangat rahasia, yaitu kunci dari sebuah kriptografi simetris. Pada algoritma ElGamal suatu plainteks yang sama akan dienkripsi menjadi cipherteks yang berbeda-beda. Hal ini dikarenakan pemilihan bilangan k yang acak. Akan tetapi, walaupun cipherteks yang diperoleh berbeda-beda, tetapi pada proses dekripsi akan diperoleh plainteks yang sama.

Mengingat masih banyaknya hal-hal yang belum dapat diimplementasikan pada penelitian ini, maka penulis berharap pembaca dapat mengkaji lebih dalam tentang kriptografi ElGamal sehingga dapat mengembangkan aplikasi pembelajaran kriptografi ini ke dalam algoritma kriptografi yang lain.

DAFTAR PUSTAKA

[1] Ariyus, Doni. 2008. Pengantar Ilmu Kriptografi. Yogyakarta : Andi Offset.

[2] Munir, Rinaldi. 2006. *Kriptografi*. Bandung : Informatika.

[3] Massandy, Danang Tri. 2009. *Algoritma Elgamal Dalam Pengamanan Pesan Rahasia.* Bandung : Institut Teknologi Bandung.

[4] Suyadi, Agus. 2008. *Manfaat Komputer Dalam Pembelajaran*. Surakarta: Universitas Muhammadiyah Surakarta

[5] Ifanto, Mukhammad. 2009. Metode Enkripsi Dan Dekripsi Dengan Menggunakan Algoritma Elgamal. Bandung: Institut Teknolgi Bandung.

[6] Ariwibowo, Eko. 2008. Aplikasi Pengamanan Dokumen Office Dengan Algoritma Kriptografi Kunci Asimetris ElGamal. Yogyakarta : Universitas Ahmad Dahlan Yogyakarta.

[7] Oppliger, Rolf. 2005. *Contemporary Cryptography*. USA: Artech House, Inc.

[8] Talbot, Jhon dan Dominic Welsh. 2006. Complexity and Cryptography. USA : Cambridge University Press.

[9] Menezes, Oorcshot, and Vanstone. 1996. *Handbook of Applied Cryptography.* USA : CRC Press, Inc.

[10] Schneier, Bruce. 1996. Applied Cryptography, Second Edition : Protocol, Algorithms and Source Code in C. John Wiley and Sons, Inc.