ALGORITMA KRIPTOGRAFI KUNCI PUBLIK ELGAMAL UNTUK KEAMANAN PESAN SMS (*SHORT MESSAGE SERVICE*) BERBASIS ANDROID

Islamiyah

Universitas Mulawarman; Jln Gunung Kelua, Telpon. (0541) 735133
Program Studi Teknik Informatika, Universitas Mulawarman, Samarinda
Islamiyah1601@yahoo.co.id

Abstrak

Beberapa tahun terakhir ini, terjadi perkembangan yang pesat pada teknologi pesan seluler (ponsel). Salah satunya adalah mulai bermunculan ponsel pintar dengan berbagai fitur dan memiliki sistem operasi kompleks layaknya komputer. Berbagai sistem operasi untuk ponsel pun bermunculan, diantaranya yang cukup dikenal luas adalah android. Sekalipun ponsel pintar memiliki berbagai fitur, fitur lama seperti Layanan Pesan Singkat atau lebih dikenal dengan Short Message Service (SMS) masih tetap ramai digunakan. Namun dengan fitur SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS. Kriptografi merupakan salah satu solusi yang dapat dimanfaatkan dan dikembangkan dalam menghadapi permasalahan tentang keamanan pesan SMS. Dengan melakukan enkripsi pada pesan SMS, maka kemanan pesan SMS akan lebih terjaga dan aman. Kriptografi memiliki banyak teknik dalam melakukan pengenkripsian pesan SMS dan salah satu yang memiliki tingkat keamanan yang tinggi dan tingkat kesulitan dalam pemecahannya adalah algoritma Elgamal. Metode ElGamal pesan dienkripsi dan dekripsi dengan menggunakan dua kunci yaitu privat dan kunci publik.

Kata kunci : kriptografi, pesan SMS, Elgamal

1. PENDAHULUAN

Perkembangan teknologi pada zaman sekarang ini tidak dipungkiri sangatlah cepat, khusus teknologi informasi salah satunya telpon seluler. Fitur dan kecanggihan pada telpon seluler mulai bermuncul sampai dengan adanya yang disebut smartphone, yang memiliki berbagai fungsiseperti multimedia, multiplayer games, transfer data, video streaming dan lain-lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponselpun bermunculan, diantaranya yang cukup dikenal luas adalah pada platform smartphone khususnya Android.

Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pengiriman data berupa pesan singkat melalui *Short Message Service* (SMS). Terkadang ada kalanya informasi yang kita kirim melalui SMS bersifat rahasia. Alternatif untuk merahasiakan data pesan singkat adalah dengan menerapkan algoritma kriptografi.

Kriptografi dapat diartikan sebagai teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentifikasi [5]. Kriptografi terbagi menjadi dua proses utama yaitu enkripsi dan dekripsi. Enkripsi merupakan proses merahasiakan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus, sedangkan dekripsi adalah proses pengembalian data hasil enkripsi.

Salah satu algoritma yang digunakan untuk *Enkripsi* dan dibahas dalam penelitian adalah algoritma ElGamal. Algoritma ini menekankan pada permasalahan Algoritma diskrit [3]. Dengan permasalahan tersebut maka chiperteks hasil enkripsi ElGamalakan sangat sulit di kriptanalis. Matematika diskrit yang dimaksud dalam kriptografi Elgamal adalah, mencari sebuah bilangan pangkat (x), pada sebuah bilangan bulat (g). Dimana bilangan tersebut *kongkruen* dengan bilangan bulat lainnya (y) jika di mod dengan bilangan p (bilangan prima).

Kerumitannya terletak pada masalah diskrit karena melibatkan bilangan prima p sebagai variabel modulo dan x adalah bilangan yang dicari berupa bilangan pangkat.

Ada beberapa penelitian sebelumnya yang mendasari adanya penelitian ini. Penelitian pertama Andi Riski Alvianto, dkk. (2015). Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android. Penelitian ini bertujuan untuk melakukan pengamanan pesan sms. Hasil dari penelitian ini berupa aplikasi ini dapat melakukan pengamanan terhadap pesan pada SMS dengan menggunakan algoritma RSA [1]. Penelitian kedua Faqihuddin Al-Anshori, dkk. (2014)Implementasi Algoritma Kriptografi Kunci Publik Elgamal untuk Proses Enkripsi dan Dekripsi Guna Pengamanan File Data.Penelitian ini menghasilkan aplikasi Kriptografi untuk pengamanan File data dengan menggunakan algoritma Elgamal kunci public untuk proses enkripsi dan dekripsi.[4]

METODE PENELITIAN

Proses Enkripsi ElGamal

Langkah proses enkripsi: Proses enkripsi menggunakan kunci publik (p,g,y) dan sebuah bilangan integer acak k ($k \in \{0,1,..., p-1\}$) yang dijaga kerahasiaannya oleh penerima pesan. Untuk setiap karakter dalam pesan dienkripsi dengan menggunakan bilangan k yang berbeda-beda. Satu karakter yang direpresentasikan dengan menggunakan bilangan bulat ASCII akan menghasilkan kode dalam bentuk blok yang terdiri atas dua nilai (a,b). [2]

5. Ambil sebuah karakter dalam pesan yang akan dienkripsi dan transformasi karakter tersebut ke dalam kode ASCII sehingga diperoleh bilangan bulat m. Plainteks tersebut disusun menjadi blok-blok m1, m2, ……, sedemikian hingga setiap blok merepresentasikan nilai di dalam rentang 0 (nol) sampai p-1.
6. Memilih bilangan acak k, yang dalam hal ini $0 < k < p-1$, sedemikian hingga k relative prima dengan p-1.
7. Hitung nilai a dan b dengan persamaan berikut:

$$a = gk \pmod p \ldots\ldots\ldots\ldots (4)$$
$$b = yk\, m \pmod p \ldots\ldots\ldots (5)$$

d. Diperoleh cipherteks untuk karakter m tersebut dalam blok (a,b)

e. Melakukan proses di atas untuk seluruh karakter dalam pesan termasuk karakter spasi.

Proses Dekripsi ElGamal

Dekripsi dari cipherteks ke plainteks menggunakan kunci rahasia a yang disimpan kerahasiaanya oleh penerima pesan.

Teorema :

Diberikan (p,g,y) sebagai kunci public dan x sebagai kunci rahasia pada algoritma ElGamal. Jika diberikan cipherteks (a, b), maka

$$m = b/ax \bmod p \ldots\ldots\ldots (4)$$

dengan M adalah plainteks.

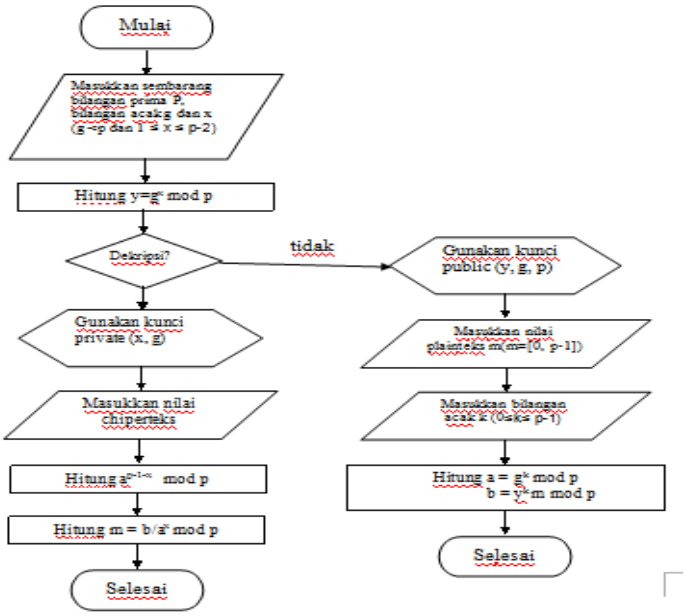
Di mana nilai

$$(ax)^{-1} = r^{-a} = rp^{-1-a} \bmod p. \ldots (5)$$

Langkah proses dekripsi:

a) Ambil sebuah blok cipherteks dari pesan yang telah dienkripsikan pengirim.
b) Dengan menggunakan a yang dirahasiakan oleh penerima, hitung nilai plainteks dengan menggunakan “persamaan (4)” dan “persamaan (5)”.

Flowchart Enkripsi dan Dekripsi



Gambar 1.*Flowchart Enkripsi dan Dekripsi ElGamal*

2. PEMBAHASAN

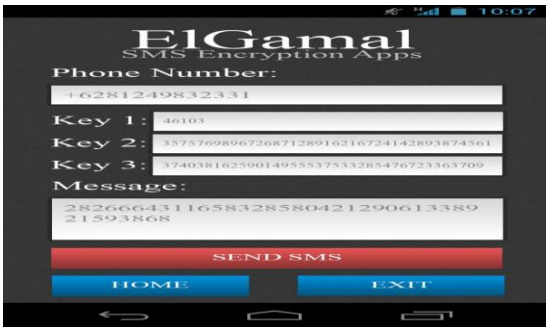
a. Menu Utama

Menu ini memperlihatkan tampilan awal dari aplikasi SMS Encryption menggunakan metode El Gamal. Di dalam menu tersebut, terlihat ada tiga opsi yang masing-masing memiliki fungsi tersendiri. SMS Encryption akan membuat si pengguna masuk pada menu untuk mengirimkan pesan yang akan dienkripsi. Sementara untuk SMS Decryption akan menampilkan pesan enrkipsi yang diterima dan perlu dilakukan dekripsi untuk membacanya, sedangkan untuk tombol Exit sendiri akan membuat pengguna keluar dari aplikasi.

Gambar 2. Menu Utama

b. SMS Encryption

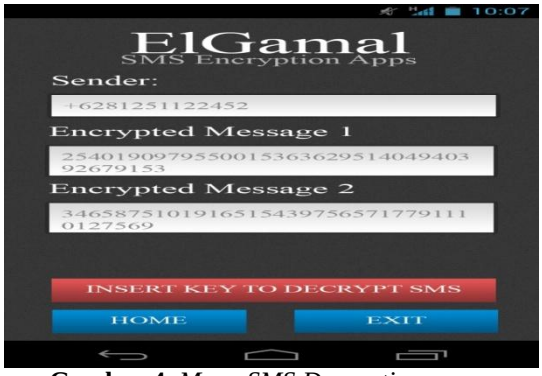
Tombol SMS Encryption di menu utama akan menampilkan format untuk mengirimkan pesan dilengkapi dengan tiga key yang harus diisi oleh si pengirim. Key tersebut merupakan kunci publik yang hanya diketahui oleh si pengirim saja. Di bagian ini, selain menuliskan pesan yang akan dienkripsi, masukkan pula nomor ponsel yang menjadi tujuan. Ketika tombol Send SMS dipilih, maka pesan secara otomatis akan dienkripsi oleh aplikasi, lalu kemudian dikirimkan kepada nomor tujuan sesuai dengan nomor yang telah diisi sebelumnya.



Gambar 3. Menu SMS Encryption

c. SMS Decryption

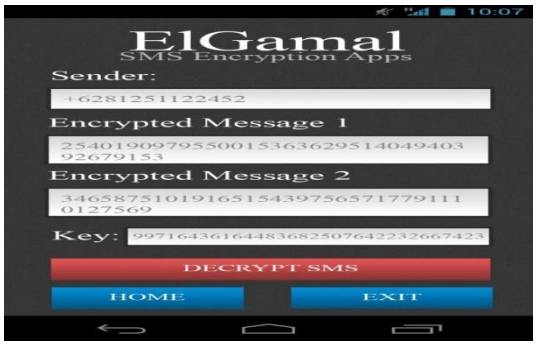
Menu utama, terdapat tombol SMS Decryption, dimana tombol tersebut akan membawa pengguna menuju ke daftar pesan yang perlu di dekripsi agar dapat dibaca. Diatas ini adalah contoh pesan yang diterima dalam bentuk terenkripsi (bukan pesan asli), dimana terdapat dua bagian pesan yang terpisah. Untuk dapat membaca pesan tersebut, diperlukan kunci private yang seharusnya telah diketahui oleh si penerima dan diberitahukan oleh si pengirim. Jika ingin melakukan dekripsi pesan tersebut, pengguna harus memilih opsi Insert Key To Decrypt SMS.



Gambar 4. *Menu SMS Decryption*

d. Insert Private Key

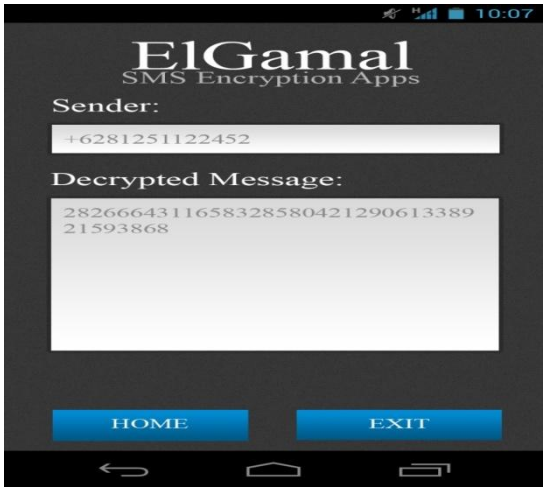
Setelah memilih opsi Insert Key to Decrypt SMS, maka pengguna harus menginputkan key private ke dalam form isian yang tampil pada form sebelumnya. Key tersebut diperlukan agar pesan yang telah terenkripsi dapat dienkripsi oleh sistem aplikasi dan teks aslinya dapat dibaca oleh si pengguna



Gambar 5.*Menu Insert Private Key*

e. Decrypted Message

Setelah meinputkan key private yang benar dan memilih opsi Decrypt SMS, maka pesan yang terenkripsi dapat ditampilkan oleh sistem dan dapat dibaca oleh si pengguna.



Gambar 6. *Menu Decryted Message*

3. Kesimpulan

1. Algoritma asimetris memiliki kunci enkripsi yang berbeda dengan kunci dekripsi. Kunci untuk enkripsi disebut dengan kunci publik sedangkan kunci untuk dekripsi disebut dengan kunci private.
2. Tingkat keamanan algoritma ini didasarkan pada kesulitan pemecahan masalah logaritma diskret pada penggandaan bilangan bulat modula prima yang besar.
3. Dapat memudahkan pengguna dalam melakukan proses pengiriman dan penerimaan pesan yang bersifat sangat penting dan rahasia.
4. Membuktikan bahwa algoritma Elgamal tidak hanya cuma digunakan untuk mengamankan data maupun digital signature, tetapi metode ini dapat diterapkan untuk proses pengiriman pesan dan penerimaan pesan berbasis SMS.

DAFTAR PUSTAKA

[1] Andi Riski Alvianto, dkk. 2015. Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android JURNAL SAINS DAN SENI ITS Vol. 4, No.1.
[2] Agus Abdullah. 2013. Aplikasi Enkripsi Pesan SMS dengan Algoritma Kriptografi *Block Chiper* DES Berbasis Android.
[3] Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi*. Andi: Yogyakarta.
[4] Faqihuddin Al-Anshori, dkk.. 2014. Implementasi Algoritma Kriptografi Kunci Publik Elgamal untuk Proses Enkripsi dan Dekripsi Guna Pengamanan File Data.JURNAL INFORMATIKA Februari 2014.
[3] Joko Dewanto, dksk. 2013. Pembuatan Aplikasi SMS Kriptografi RSA dengan Android. Forum Ilmiah Volume 10 Nomor 2.
[4] Munir, Rinaldi. 2005. *Bahan Kuliah IF3058 Kriptografi*. STEI-ITB.
[5] . 2006. *Kriptografi*. Informatika. Bandung.
[6] M. Taufiq Tamam. 2010. Penerapan Algoritma Kriptografi Elgamal untuk Pengaman

File Citra. Jurnal EECCIS Vol. IV, No.1, Juni 2010.
[7] Safaat H, Nazruddin. 2011. Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android. Penerbit Informatika: Bandung.
[8] Yudhistira Taufan. 2011. Enkripsi Email dengan Menggunakan Metode Elgamal pada Perangkat Mobile.

Biodata Penulis

Islamiyah, memperoleh gelar Sarjana Komputer (S.Kom) di Jurusan Sistem Informasi, STMIK Dipanegara Makassar dan lulus tahun 2008, memperoleh gelar Magister Komputer (M.Kom) di Jurusan Magister Teknik Informatika STMIK Amikom Jogjakarta dan lulus tahun 2013