IMPLEMENTASI KRIPTOGRAFI DENGAN METODE *ELLIPTIC CURVE CRYPTOGRAPHY* (ECC) UNTUK APLIKASI *CHATTING* DALAM *CLOUD COMPUTING* BERBASIS ANDROID

Ainur Rilo Taqwa[1)], Danang Haryo Sulaksono[2)]
[1,2]Jurusan Teknik Informatika, Fakultas Teknik Elektro dan Teknologi Informasi
Institut Teknologi Adhi tama Surabaya
email : Ainurrilo@ymail.com , danang_h_s@itats.ac.id

ABSTRACT

In general, information dissemination facilities in the current technological era can be done quickly and easily through the android application media. One of the most frequently used media for information dissemination is chatting. The problem with this research is that the chat application allows someone to send messages or files to other users who have access rights, with the risk that the data will be seen by anyone who has access rights in it. This can happen because in the chat application can see anything that is shared as long as you have access rights, but sometimes there is some data that is privacy. So it is necessary to add a means to secure this privacy data so it cannot be seen by other users. The solution to overcome this problem is a cryptographic system. One cryptographic method that provides solutions to information security problems is the Elliptic Curve Cryptography (ECC) method. Therefore this thesis proposal is to create an online system in order to implement cryptography with the Elliptic Curve Cryptography (ECC) method for Android-based chat applications. The testing process in this study using 25 image data obtained, the smallest avalanche effect value is 36.52801638, the biggest avalanche effect is 94,67749211. And obtained an average avalanche effect value of 79,8881925. The average avalanche effect that produces a large enough percentage proves that the application is running well, because the greater the percentage obtained, the better the application is running. From the above test it can be concluded that the Elliptic Curve Cryptography (ECC) algorithm method is effective for hiding data files in chat applications that are privacy.

Keywords: Cryptography, Elliptic Curve Cryptography (ECC) Algorithm, Avalanche Effect

ABSTRAK

Secara umum, fasilitas penyebaran informasi pada era teknologi yang saat ini dapat dilakukan dengan cepat dan mudah melalui media aplikasi *android*. Salah satu media yang paling sering digunakan untuk penyebaran informasi adalah *chatting*. Masalah dari penelitian ini adalah aplikasi *chatting* memungkinkan seseorang dapat mengirim pesan ataupun *file* kepada *user* lain yang telah memiliki hak akses, dengan resiko datanya akan dapat dilihat oleh siapa saja yang memiliki hak akses didalamnya. Hal ini dapat terjadi karena didalam aplikasi *chatting* tersebut dapat melihat apapun yang dibagi selama memiliki hak akses, namun terkadang ada beberapa data yang bersifat privasi. Sehingga perlu ditambahkan suatu sarana untuk mengamankan data privasi ini agar tidak dapat dilihat oleh *user* lain. Adapun solusi untuk mengatasi hal tersebut maka dibuatlah sebuah sistem kriptografi. Salah satu metode kriptografi yang memberikan solusi untuk permasalahan keamanan informasi adalah metode *Elliptic Curve Cryptography* (ECC). Oleh karena itu proposal skripsi ini untuk membuat sebuah sistem online agar dapat mengimplementasikan cryptography dengan metode Elliptic Curve Cryptography (ECC) untuk aplikasi chatting berbasis Android. Proses pengujian pada penelitian ini menggunakan 25 data citra didapatkan, nilai avalanche effect terkecil adalah 36,52801638, avalanche effect terbesar adalah 94,67749211. Dan didapatkan nilai avalanche effect rata – rata sebesar 79,8881925. Nilai rata – rata avalanche effect yang menghasilkan persentase yang cukup besar membuktikan bahwa aplikasi berjalan dengan baik, karena semakin besar persentase yang didapatkan maka semakin baik aplikasi itu berjalan. Dari pengujian diatas dapat disimpulkan bahwa metode algoritma Elliptic Curve Cryptography (ECC) ini efektif untuk menyembunyikan file data pada aplikasi chatting yang bersifat privasi.

Kata Kunci : *Kriptografi*, Algoritma *Elliptic Curve Cryptography* (ECC), *Avalanche Effect*

1. PENDAHULUAN

Secara umum, fasilitas penyebaran informasi pada era teknologi yang saat ini dapat dilakukan dengan cepat dan mudah melalui media aplikasi *android*. Salah satu media yang paling sering digunakan untuk penyebaran informasi adalah *chatting*. Aplikasi *chatting* merupakan suatu sarana untuk berkomunikasi langsung sesama pengguna *internet*. Aplikasi *chatting* saat ini tidak hanya terbatas berupa data teks tapi juga berupa gambar (*image*). (Khadim,2015).

Secara khusus, aplikasi chatting merupakan suatu pesan *instant* ataupun *instant messaging* di sebuah teknologi jaringan komputer yang mengijinkan pemakainya untuk mengirimkan pesan ke pengguna lain yang tersambung dalam sebuah jaringan komputer ataupun internet.

Masalah dari penelitian ini adalah aplikasi chatting memungkinkan seseorang dapat mengirim pesan ataupun file kepada user lain yang telah memiliki hak akses, dengan resiko datanya akan dapat dilihat oleh siapa saja yang memiliki hak akses didalamnya. Hal ini dapat terjadi karena didalam aplikasi chatting tersebut dapat melihat apapun yang dibagi selama memiliki hak akses, namun terkadang ada beberapa data yang bersifat privasi. Sehingga perlu ditambahkan suatu sarana untuk mengamankan data privasi ini agar tidak dapat dilihat oleh user lain.

Adapun solusi untuk mengatasi hal tersebut maka dibuatlah sebuah sistem kriptografi. Salah satu metode kriptografi yang memberikan solusi untuk permasalahan keamanan informasi adalah metode *Elliptic Curve Cryptography* (ECC). Metode ECC adalah metode kriptografi yang memberikan solusi kunci publik secara independen / bebas.

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka dapat dirumuskan permasalahan. Yaitu bagaimana mengimplementasikan *cryptography* dengan metode *Elliptic Curve Cryptography* (ECC) untuk aplikasi *chatting* berbasis *android* dan bagaimana performa komputasi metode algoritma *Elliptic Curve Cryptography* (ECC) untuk aplikasi *chatting*.

Berdasarkan rumusan masalah diatas maka tujuan penelitian ini adalah untuk Menjaga keamanan *file* data pada aplikasi *chatting* menggunakan algoritma *Elliptic Curve Cryptography* (ECC) berbasis android. Dan Menyembunyikan *file* data pada aplikasi *chatting* yang bersifat privasi menggunakan algoritma *Elliptic Curve Cryptography* (ECC). Manfaat yang didapatkan pada penelitian ini adalah mengamankan *file* data *online* yang bersifat pribadi pada aplikasi *chatting*.

2. Tinjauan Pustaka

2.1. Kriptografi

Kriptografi berasal dari gabungan dua kata yaitu "*Crypto*" yang berarti rahasia dan "*graphy*" yang berarti tulisan. Dalam bahasa komputasi kriptografi diartikan sebagai ilmu dan seni untuk menjaga keamanan data. Ahli kriptografi disebut kriptografer. (Jaya, 2017).

2.2 Algoritma *Elliptic Curve Cryptography* (ECC)

Eliptic Curve Cryptography (ECC) merupakan sistem kriptografi kunci publik yang memanfaatkan persamaan kurva eliptik. Algoritma ini dirancang dan diajukan oleh Neal Koblitz dan Victor S. Miller. Penyebab utamanya adalah karena dengan menggunakan kunci yang jauh lebih kecil atau pendek, *Eliptic Curve Cryptography* (ECC) tetap dapat memberikan tingkat keamanan yang sama dengan algoritma asimetrik lainnya yang menggunakan kunci yang lebih besar. Dengan ukuran kunci yang lebih kecil dan tingkat keamanan yang sama tinggi, implementasi *Eliptic Curve Cryptography* (ECC) menjadi lebih efisien. (Edy, 2017).

2.3 Arsitektur Platform Android

Arsitektur lain yang tak kalah penting dalam proses perancangan sistem *cloud computing* adalah *Application Programming Interface* (API). Menurut Lew Tucker, Chief Technology Officer dari Sun Microsystems *Cloud Computing Division*, API merupakan aspek yang seringkali dilupakan oleh para pengguna layanan *cloud computing*. Aplikasi yang tersedia pada *cloud computing* dapat diakses melalui Internet.

2.4 Java Android

Java adalah bahasa berorientasi objek yang dapat digunakan untuk pengembangan aplikasi mandiri, aplikasi berbasis *internet*, serta aplikasi untuk perangkat - perangkat cerdas yang dapat berkomunikasi lewat internet atau jaringan komunikasi. Dalam java ada 2 (dua) jenis program berbeda, yaitu aplikasi dan *applet*.

2.5 Android SDK (*Software Development Kit*)

Andrioid SDK adalah *tools* API (*Application Programing Interface*) yang diperlukan untuk memulai mengembangkan aplikasi pada *platform Android* menggunakan bahasa pemrograman Java.

2.6 Pengujian

Untuk melakukan pengujian pada penelitian ini menggunakan beberapa parameter yang digunakan. Parameter yang digunakan adalah *Avalanche Effect*. *Avalanche Effect* adalah salah satu cara untuk mengetahui tingkat efektifitas algoritma kriptografi dari *file* yang dienkripsi. Dengan ketentuan bahwa algoritma itu semakin baik bila memiliki nilai *Avalanche Effect* yang tinggi. *Avalanche Effect* dapat dihitung dengan menggunakan rumus 1.

$$Avalanche\ Effect = \frac{jbt}{jbc} \times 100\% \quad \text{----------(1)}$$

Keterangan:

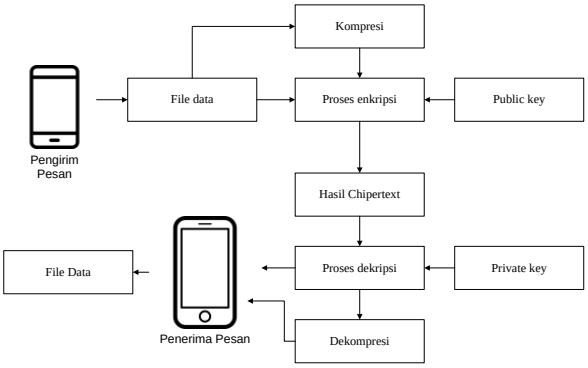
jbt : Jumlah bit yang terbaikdalam chipertext

jbc : Jumlah bit keseluruhan dalam ciphertext

3. METODE PENELTIAN

3.1 Gambaran Umum

Dalam penelitian ini diterapkan sistem menggunakan algoritma *Elliptic Curve Cryptography* (ECC). Dimana hal ini berguna untuk mengenkripsi dan dekripsi file citra pada saat chatting.

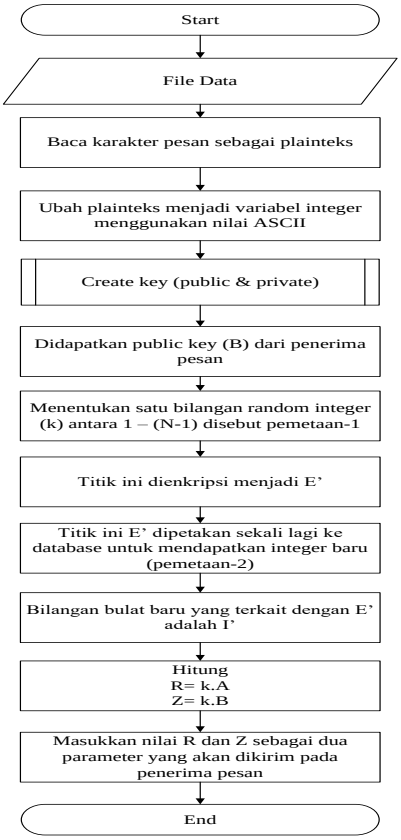


Gambar 1. Skema Perancangan Aplikasi

Gambar 1 diatas menjelaskan tentang skema rancangan aplikasi enkripsi dan dekripsi algoritma *Elliptic Curve Cryptography* (ECC). Dimana sistem ini berbasis *android* sehingga untuk menggunakannya perlu menggunakan *smartphone*. Dimana salah satu komputer akan bertindak sebagai *client* ataupun *server*, *client* sebagai penerima file data. File data yang dikirimkan oleh *server* harus di enkripsikan terlebih dahulu sebelum dikirim ke *client*. Dengan demikian meskipun file data terbaca oleh pihak lain yang berusaha membacanya akan sulit untuk memahaminya. Selain harus mendekripsikannya, tentu metode dalam pemecahannyapun hanya akan dipahami oleh *client* dan *server*.

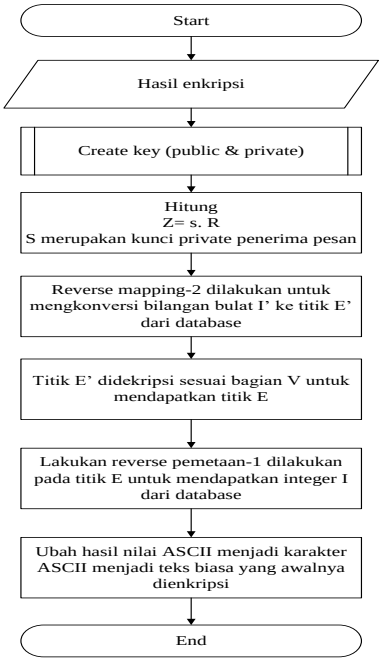
3.2 Rancangan dan Pembangunan

Tahap ini menjelaskan tentang prosedur dan proses apa saja yang akan dilakukan oleh aplikasi, alur proses, serta tampilan dasar aplikasi. Alur proses dalam hal ini berbentuk flowchart dan perhitungan manual dari metode yang digunakan. *Flowchart* dari sistem yang dibangun dapat dilihat pada gambar 3.2.



Gambar 2. Flowchart Enkripsi Algoritma ECC

Gambar 2 dibawah menjelaskan tentang alur enkripsi algoritma *Elliptic Curve Cryptography* (ECC). Proses pertama yang dilakukan adalah dengan menginputkan *file* data yang akan di enkripsi. Kemudian baca *file* data sebagai *plainteks*, untuk diubah menjadi variabel *integer* menggunakan nilai ASCII. Kemudian lakukan proses *create key* (*public* & *private*), maka akan didapatkan *public key* (B) dari penerima pesan. Selanjutnya menentukan satu bilangan *random integer* (k) antara 1 – (N-1) disebut pemetaan-1. Titik yang dipilih tadi selanjutnya dienkripsi menjadi E'. titik ini E' dipetakan sekali lagi ke *database* untuk mendapatkan *integer* baru yang disebut pemetaan-2. Lalu bilangan bulat baru yang terkait dengan E' adalah I' didapatkan. Kemudian menghitung nilai R dengan mengalikan nilai k dengan A (titik awal). Dan menghitung nilai Z dengan mengalikan nilai k dengan B (*public key*). Terakhir, masukkan nilai R dan Z sebagai dua parameter yang akan dikirim pada penerima pesan.

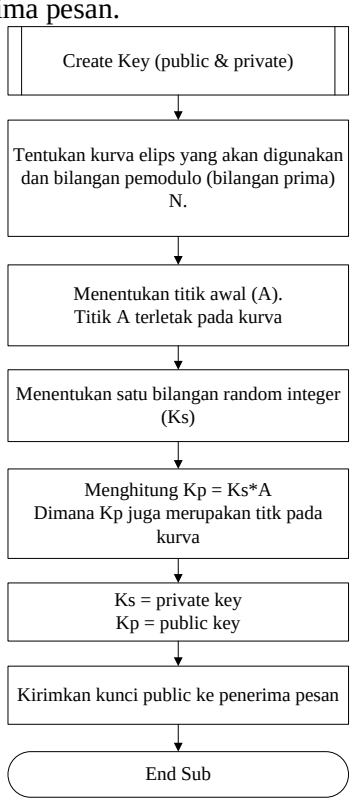


Gambar 3. Flowchart Dekripsi Algoritma ECC

Gambar 3 dibawah menjelaskan tentang alur dekripsi algoritma *Elliptic Curve Cryptography* (ECC). Proses pertama yang dilakukan adalah dengan menginputkan hasil enkripsi. Kemudian dilakukan proses *create Key (public & private)*. Kemudian hitung nilai Z dengan mengalikan nilai s dengan R, dimana s adalah kunci *private* penerima pesan. Selanjutnya dilakukan proses *reverse* mapping-2 untuk mengkonversi bilangan bulat I' ke titik E' dari *database*. Lalu, titik E' didekripsikan sesuai bagian V untuk mendapatkan titik E. Setelah itu lakukan *reverse* pemetaan-1 pada titik E untuk mendapatkan *integer* I dari *database*. Kemudian ubah hasil nilai ASCII menjadi karakter ASCII menjadi teks biasa yang awalnya dienkripsi.

Gambar 4. menjelaskan tentang alur *create key* algoritma *Elliptic Curve Cryptography* (ECC). Proses pertama yang dilakukan adalah dengan menentukan kurva elips yang akan digunakan dan bilangan pemodulo (bilangan prima) N. kemudian, menentukan titik awal (A) titik A terletak pada kurva. Selanjutnya, menentukan satu bilangan random integer (Ks). Setelah itu menghitung nilai Kp dengan mengalikan nilai Ks dengan titik awal (A). dimana Kp juga merupakan titik

pada kurva. Terakhir didapatkan nilai Ks sebagai *private key* dan nilai Kp sebagai *public key*. Selanjutnya kirimkan kunci ke penerima pesan.



Gambar 4. *Flowchart* Enkripsi Algoritma *Shannon - Fano*

4. HASIL DAN PEMBAHASAN

Pengujian ini dilakukan untuk mendapatkan hasil data dari keseluruhan proses, baik proses enkripsi maupun dekripsi pada algoritma *Elliptic Curve Cryptography* (ECC). Untuk melakukan pengujian pada penelitian ini dengan menggunakan beberapa parameter yang digunakan. Parameter yang digunakan adalah *Avalanche Effect*. Pada penelitian ini telah dilakukan uji coba dengan menggunakan 25 data citra dengan cara jumlah bit terbaik dibagi dengan jumlah bit keseluruhan.

Tabel 1. Perhitungan Pengujian Sistem

No	Jumlah Bit Terbaik	Jumlah Bit Keseluruhan	*Avalanche Effect* (%)
1	2096	2598	80.67744419
2	4786	5597	85.51009469
3	19018	25188	75.50420835
4	3491	4125	84.63030303
5	2215	2474	89.53112369
6	24830	56303	44.10066959
7	18509	23587	78.47119176
8	6559	7056	92.95634921
9	120987	331217	36.52801638
10	27900	36640	76.14628821
11	4302	5242	82.06791301
12	31275	45413	68.8679453
13	53850	63650	84.60329929
14	27228	30524	89.20193946
15	72275	103920	69.5486913
16	1574	1876	83.90191898
17	5152	5818	88.55276727
18	4198	4434	94.67749211
19	2629	2811	93.52543579
20	62045	95020	65.29677963
21	58321	65517	89.01659111
22	12207	14099	86.58060855
23	66300	79123	83.7935872
24	43377	49865	86.98886995
25	53162	61441	86.52528442
Rata - rata			79,8881925

Tabel 1 adalah tabel pengujian data untuk mendapatkan nilai *Avalanche Effect*. Dari hasil pengujian diatas maka didapatkan nilai *avalanche effect* terkecil adalah 36,52801638, *avalanche effect* terbesar adalah 94,67749211. Dan didapatkan nilai *avalanche effect* rata – rata sebesar 79,8881925. Nilai rata – rata *avalanche effect* yang menghasilkan persentase yang cukup besar membuktikan bahwa aplikasi berjalan dengan baik, karena semakin besar persentase yang didapatkan maka semakin baik aplikasi itu berjalan.

Avalanche Effect ini menunjukkan bahwa suatu metode cocok digunakan untuk menyelesaikan masalah yang sedang terjadi saat ini. Dengan kata lain, bahwa *avalanche effect* ini berfungsi untuk mengetahui apakah suatu metode sudah efektif atau belum dalam sebuah penelitian. Dari pengujian diatas dapat disimpulkan bahwa metode algoritma *Elliptic Curve Cryptography* (ECC) ini efektif untuk menyelesaikan masalah enkripsi dan dekripsi sebuah citra digital. Hal ini dikarenakan bahwa sebuah algoritma yang baik memiliki *avalanche effect* tinggi.

5. Kesimpulan

Dari hasil analisa yang telah dilakukan dapat diambil kesimpulan sebagai berikut :

1. Dari hasil percobaan sebanyak 25 data citra didapatkan, nilai *avalanche effect* terkecil adalah 36,52801638, *avalanche effect* terbesar adalah 94,67749211. Dan didapatkan nilai *avalanche effect* rata – rata sebesar 79,8881925. Nilai rata – rata *avalanche effect* yang menghasilkan persentase yang cukup besar membuktikan bahwa aplikasi berjalan dengan baik, karena semakin besar persentase yang didapatkan maka semakin baik aplikasi itu berjalan. Dari pengujian diatas dapat disimpulkan bahwa metode algoritma *Elliptic Curve Cryptography* (ECC) ini efektif untuk menyembunyikan *file* data pada aplikasi *chatting* yang bersifat privasi.

6. DAFTAR PUSTAKA

Damanik, Putri S E A. (2019). ***"Implementasi Algoritma Elliptic Curve Cryptography (ECC) Untuk Penyandian Pesan Pada Aplikasi Chatting Client Server Berbasis Desktop"***. Jurnal Riset Komputer. Vol. 6, No. 4. ISSN 2407 – 389X(Media Cetak).

Edy Budi Harjono Sibarani M.Kom, Prof. Dr. Muhammad Zarlis, Rahmat Widya Sembiring M. PhD. (2017)."***Analisis Kriptografi Sistem Algoritma AES dan Elliptic Curve Cryptography (ECC) Untuk Keamanan Data***", Info Tekjar (Jurnal Nasional Informatika dan Informasi Jaringan). Vol. 1, No. 2. e-ISSN: 2540 – 7600, p-ISSN : 2540 – 7597.

Jaya Santoso Sirait, R. Rumani M., Marisa W. Paryanto. (2017)."***Implementasi Kriptosystem menggunakan metode algoritma ECC dengan fungsi MD5 pada sistem database ticketing online***"**,** e-Proceeding of Engineering. Vol. 4, No. 3.

Kadhim, Dr. Alaa. Khalaf, Sura. (2015). "***New Approach for Security Chatting in Real Time***", International Journal of Emerging Trends & Teknology in Computer Science (IJETTCS). Volume 4, Issue 3. ISSN 2278 – 6856.

Kolhekar, Mrs. Megha. Jadhav, Mrs. Anita. (2011). "***Implementation Of Elliptic Curve Cryptography On Text And Image***"**,** International Journal oF Enterprise Computing and Business systems. ISSN (Online) 2230 – 8849.

Laksana, Tri Ginanjar. (2018)."***Penggunaan Algoritma ECC (Elliptic Curve Cryptography) sebagai Teknik Pengamanan Transmisi Pada Query Database***"**,** Jurnal Teknik Informatika. Institut Teknologi Telkom Purwokerto.

Nawagusti, Vera Apriliani. (2018)."***A Review on Elliptic Curve Cryptography and Variant***"**,** International Research Journal of engineering an teknology (IRJET). Vol.05 Issue : 05.

Surfina Adilah, R. Rumani M. Marisa W. Paryasto (2017). "***Implementasi Kriptosystem menggunakan metode algoritma ECC dengan fungsi hash SHA -256 pada sistem tecketing online***"**,** e-Proceeding of Engineering. Vol. 4, No. 3.