Implementasi Kriptografi dengan Metode *Elliptic Curve Cryptography* (ECC) untuk Aplikasi *Chatting* Berbasis Android

Danang H. Sulaksono[1*], Citra N. Prabiantissa[1], Gusti E. Yuliastuti[1], Ainur R. Taqwa[1]

Teknik Informatika, Fakultas Teknik Elektro dan Teknologi Informasi,
Institut Teknologi Adhi Tama Surabaya[1]
e-mail: dananghs@itats.ac.id

ABSTRACT

In this technological era, information dissemination facilities can be done quickly and easily. One of the most frequently used media for disseminating information is a chat application. Chat application is a means to communicate directly with other internet users. Chat applications are currently not only limited to text data but also in the form of images. The problem of this research is that the chat application allows someone to send messages or files to other users who already have access rights, with the risk that the data will be seen by anyone who has access rights in it. Therefore, there is a technique that can overcome network security problems, namely the Elliptic Curve Cryptography (ECC) method. The ECC method is a cryptographic method that provides an independent or free public key solution. From the experimental results, 25 image data were obtained, the smallest Avalanche Effect value was 36.52801638, the largest Avalanche Effect value was 94.67749211. Then the average Avalanche Effect value is 79.8881925.

Kata kunci: Cryptography, *Elliptic Curve Cryptography* (ECC), Android, *Chatting Application*

ABSTRAK

Pada era teknologi seperti sekarang ini, fasilitas penyebaran informasi dapat dilakukan dengan cepat dan mudah. Salah satu media yang paling sering digunakan untuk penyebaran informasi adalah aplikasi *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. Permasalahan 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. Maka dari itu, terdapat suatu teknik yang dapat mengatasi permasalahan keamanan jaringan yaitu metode *Elliptic Curve Cryptography* (ECC). Metode ECC adalah metode kriptografi yang memberikan solusi kunci publik secara independen atau bebas. Dari hasil percobaan sebanyak 25 data citra didapatkan, nilai *Avalanche Effect* terkecil adalah 36.52801638, nilai *Avalanche Effect* terbesar adalah 94.67749211. Kemudian didapatkan nilai *Avalanche Effect* rata-rata sebesar 79.8881925.

Kata kunci: Kriptografi, *Elliptic Curve Cryptography* (ECC), Android, Aplikasi *Chatting*

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) (Kadhim, 2015).

Secara khusus, aplikasi *chatting* merupakan suatu pesan instan 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. Aplikasi *chatting* juga memiliki fasilitas lain yakni dapat berbagi data kepada seluruh pengguna yang tersedia dimana dapat diakses oleh banyak pengguna. Fasilitas ini merupakan fasilitas komunikasi antara *client* dengan *server*, agar *client* mendapatkan akses untuk melihat dan mengungguh *file* pada aplikasi *chatting* tersebut (Damanik, 2019).

Permasalahan 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 mekanisme untuk mengamankan data privasi ini agar tidak dapat dilihat oleh *user* lain.

Adapun solusi untuk mengatasi permasalahan tersebut yakni dengan menerapkan kriptografi. Kriptografi adalah suatu ilmu yang dapat digunakan untuk untuk mengamankan data, sehingga sangat tepat untuk mengatasi permasalahan diatas (Patil, 2018). Dimana kriptografi juga digunakan untuk mencegah terjadinya penyadapan informasi, dimana hal ini juga sangat penting bagi aplikasi *chatting* . Kriptografi juga berfungsi pada beberapa aspek penting seperti, kerahasiaan, integritas, dan keaslian. Dimana hal tersebut untuk memastikan keamanan informasi, informasi yang tidak berubah, dan perimiman informasi pada pihak yang sah / asli (Jaya, 2017).

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 atau bebas (Laksana, 2018). Selain itu, metode ECC memiliki kelebihan yaitu tingkat keamanannya lebih bagus dibandingkan metode kriptografi yang lain dengan kunci yang jauh lebih pendek. Metode ECC akan melakukan proses enkripsi terlebih dahulu sebelum mengirimkan informasi melalui aplikasi *chatting* (Sarfina, 2017). Hasil dari enkripsi inilah yang meski terbaca oleh pihak lain maka makna dari pesan ataupun gambar yang telah dienkripsikan tidak akan dapat dimengerti oleh pihak lain yang berusaha membacanya. Hanya dengan mendekripsikan pesan ataupun gambar tersebut lah cara agar dapat membaca dan memahami makna dari pesan dan gambar yang telah dienkripsikan tersebut (Kolhekar, 2011).

Hal yang sama juga dilakukan seperti pada *file data–text* yang sangat rentan dalam fleksibilitas dan mobilitas yang sangat tinggi. Sehingga butuh suatu mekanisme untuk mengamankan data–text. Algoritma enkripsi berperan penting dalam sekuritas data–text digital. Di sisi lain, perkembangan pemecahan kode enkripsi juga ikut berkembang sehingga tidak cukup mengamankan data–text digital. Karenanya dibutuhkan beberapa level algoritma atau yang dapat juga disebut multiple encryption untuk mengamankan data–text tersebut (Danang, 2016).

Berdasarkan latar belakang tersebut, penulis membuat sebuah sistem *online* agar dapat mengimplementasikan cryptography dengan metode *Elliptic Curve Cryptography* (ECC) untuk aplikasi *chatting* berbasis Android.

TINJAUAN PUSTAKA

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).

Algoritma *Elliptic Curve Cryptography* (ECC)

Elliptic 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, 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 ECC menjadi lebih efisien (Edy, 2017).

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.

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*.

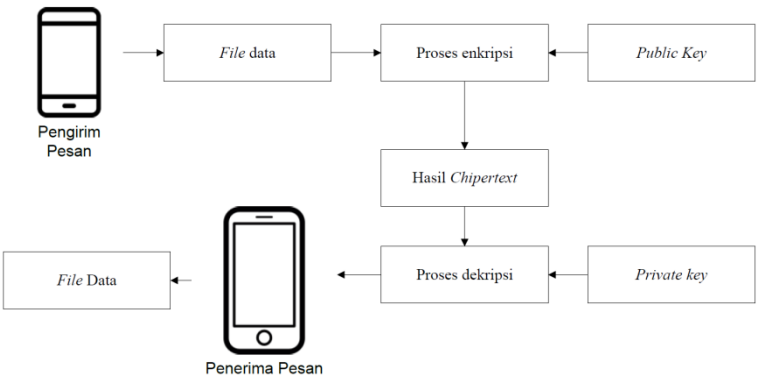
Android *Software Development Kit* (SDK)

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

METODE

Gambaran Umum

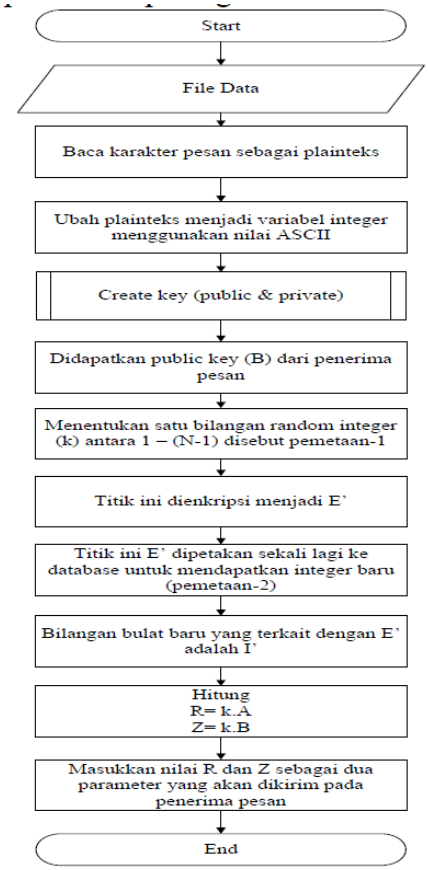
Dalam penelitian ini diterapkan sistem menggunakan algoritma Elliptic Curve Cryptography (ECC). Dimana hal ini berguna untuk mengenkripsi dan dekripsi file citra pada saat chatting.



Gambar 1 menunjukkan 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* dan *server* sebagai pengirim *file data*. *File data* yang dikirimkan oleh *server* harus dienkripsikan 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 kedua belah pihak saja yakni *client* dan *server*.

Rancangan dan Pembangunan

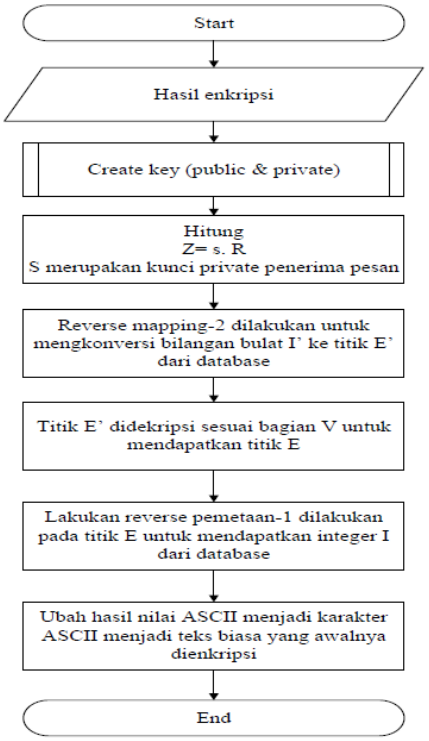
Tahap ini menjelaskan tentang prosedur dan proses apa saja yang akan dilakukan oleh aplikasi, alur proses, serta tampilan dasar aplikasi. Alur proses dalam hal ini berbentuk flowchart dan perhitungan manual dari metode yang digunakan. Flowchart dari sistem yang dibangun dapat dilihat pada Gambar 2.



Gambar 1 *Flowchart* Enkripsi Algoritma ECC

Pada Gambar 2 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 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.

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	JumlahBit Terbaik	Jumlah Bit Keseluruhan	*AvalancheEffect* (%)
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 merupakan 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.

KESIMPULAN

Dari hasil percobaan sebanyak 25 data citra didapatkan, nilai *Avalanche Effect* terkecil adalah 36.52801638, nilai *Avalanche Effect* terbesar adalah 94.67749211. Kemudian 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.

DAFTAR PUSTAKA

[1] 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,

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

[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.

[4] 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.

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

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

[7] 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.