PENERAPAN *END-TO-END ENCRYPTION* DENGAN METODE SUPER *ENCRYPTION* UNTUK KERAHASIAAN CITRA DIGITAL PADA APLIKASI *INSTANT MESSAGING*

Feri Fahrianto, Arini, Addinul Kitanggi

Teknik Informatika, Fakultas Sains dan Teknologi
Universitas Islam Negeri Syarif Hidayatullah Jakarta
feri.fahrianto@uinjkt.ac.id, arini@uinjkt.ac.id, addinul@mhs.uinjkt.ac.id

ABSTRAK

Instant Messaging merupakan media komunikasi pengiriman pesan yang marak digunakan untuk saat ini sebagai pengganti telepon dan SMS. Salah satu fitur pada layanan *instant messaging* yang populer adalah fitur pengiriman citra digital. Ada potensi ancaman keamanan pada *instant messaging* berbentuk pencurian data citra digital yang dikirim melalui jaringan layanan *instant messaging* dan juga pencurian data pada *database* yang tersimpan pada *server* pihak ketiga. Solusiyang dapat dilakukan untuk hal ini adalah dengan menggunakan *end-to-end encryption* (Andre 2009). *End-to-end encryption* (E2EE) adalah suatu mekanisme komunikasi dimana orang yang bisa membaca pesannya hanyalah orang yang sedang berkomunikasi tersebut. Algoritma enkripsi yang digunakan dalam implementasi E2EE bisa bervariasi. Dalam penelitian ini algoritma enkripsi yangdigunakan adalah *super encryption* dengan menggabungkan *playfair cipher* dengan *Vigenere cipher* yangcukup efektif untuk digunakan pada *mobile phones* (Setyaningsih et al. 2012). Untuk itu, penulis merancang dan membangung aplikasi *instant messaging* yang dapat berjalan pada *platform mobile* Android yang dapat mengenkripsi dan mengirim citra digital yang berguna untuk meningkatkan keamanan pada layanan*instant messaging*.

Kata Kunci:*instant messaging, end-to-end encryption, super encryption, multiple encryption, vigenere cipher, playfair cipher, extreme programming*

ABSTRACT

Instant Messaging is the communication media messaging rapidly adopted for the moment as a substitute for phone and SMS. One of the features of the popular instant messaging service is a feature of digital image delivery. There are potential security threats in the form of instant messaging theft of digital image data that is sent over the network instant messaging services as well as theft of data on a database stored on third party servers. Solutions that can be done to accomplish this is by using end-to-end encryption (Andre 2009). End-to-end encryption (E2EE) is a communications mechanism where people can read the message only the people who are communicating. The encryption algorithm used in the implementation of E2EE can vary. In this study, the encryption algorithm used is super encryption by combining the Playfair cipher and Vigenere cipher that is effective enough to be used on mobile phones (Setyaningsih et al. 2012). Therefore, the author designed and to bring instant messaging applications that can run on the Android mobile platform that can encrypt and send a digital image that is useful to enhance the security of instant messaging services.

Keywords: *instant messaging, end-to-end encryption, super encryption, multiple encryption, vigenere cipher, Playfair cipher, extreme programming*

I.PENDAHULUAN

Instant Messaging (IM) merupakan media komunikasi pengiriman pesan yang marak digunakan untuk saat ini sebagai pengganti telepon dan SMS. Sudah menjadi hal yang lazim untuk layanan IM saat ini memiliki fitur untuk mengirim foto atau citra digital antar sesama pengguna. Global Web Index, pada tahun 2014, menyatakan bahwa 68% pengguna perangkat *mobile* lebih memilih *mobile instant messaging* daripada SMS dengan alasan kemudahan dalam berbagi foto. Sumber yang sama juga menyebutkan bahwa hampir dari dua pertiga pengguna menyatakan fitur pengiriman foto, video dan pesan suara masuk ke dalam tiga fitur teratas yang dianggap penting. Dua fitur teratas setelahnya adalah fitur terkait dengan privasi pengguna, yaitu fitur yang membuat percakapan yang mereka hapus benar-benar terhapus dan tidak tersimpan di tempat lain yang mereka tidak ketahui dan fitur yang membuat percakapan mereka hanya tersimpan di perangkat mobile mereka dan tidak tersimpan dalam *server* pihak ketiga. Hal ini menunjukkan bahwa sebagian pengguna *mobile instant messaging* peduli terhadap kerahasiaan informasi yang mereka pertukarkan melalui layanan *instant messaging*.

Bentuk ancaman keamanan pada *instant messaging* terkait dengan hal-hal yang penulis sampaikan pada paragraf sebelumnya adalah pencurian data citra digital yang dikirim melalui layanan *instant messaging*. Andre (2009) menyatakan bahwa pencurian dapat dilakukan dibeberapa titik diantaranya adalah pencurian data yang tersimpan pada *server* penyedia layanan *instant messaging* dan pencurian data saat dalam jaringan (*eavesdropping/snooping*). Salah satu cara untuk menghindari hal ini adalah dengan melakukan enkripsi pada data sebelum pengiriman. TLS/SSL merupakan teknologi yang umum digunakan untuk enkripsi kanal komunikasi antara *client* dan *server*. Namun itu belum cukup karena data yang tersimpan pada *server* tetap dalam keadaan tidak terenkripsi. Artinya *administrator server* dapat mengetahui semua data yang dikirim pengguna yang ada pada *server* tersebut. Solusi yang dapat dilakukan adalah dengan menggunakan *end-to-end encryption* (Andre et al. 2009).

II.DASAR TEORI

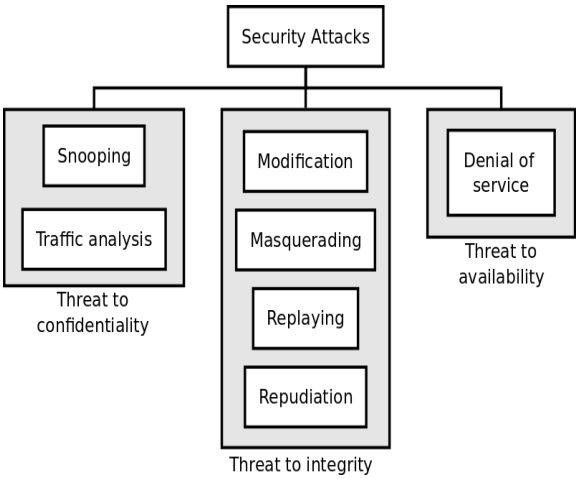
2.1. Keamanan Data dan Informasi

Forouzan (2008) membagi tujuan keamanan menjadi tiga yang dalam bukunya disebut dengan *security goals* yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Stallings (2011) juga menjelaskan tentang tiga tujuan keamanan data dan informasi serta layanan komputasi yaitu:

1. *Confidentiality*:mempertahankan pembatasan wewenang akses dan keterbukaan suatu informasi, termasuk sarana untuk melindungi privasi pribadi dan informasi kepemilikan. Hilangnya *confidentiality* adalah terungkapnya suatu informasi tanpa izin.
2. *Integrity*: menjaga suatu informasi dari modifikasi dengan cara yang tidak dibenarkan atau pengrusakan. Hilangnya *integrity* adalah modifikasi yang tidak sah atau perusakan terhadap suatu informasi.
3. *Availability*: memastikan suatu informasi dapat diakses dan digunakan pada saat dibutuhkan. Hilangnya *availability* adalah adanya gangguan pada akses atau penggunaan suatu informasi atau sistem informasi.

2.2. Ancaman Keamanan

Forouzan (2008) membagi macam-macam *security attack* berdasarkan kaitannya dengan *security goals* seperti pada gambar di bawah ini:



Gambar 1. Hubungan serangan dengan tujuan keamanan

Snooping adalah mengakses tanpa izin atau melakukan penyadapan pada suatu data. Contohnya, jika sebuah *file* yang berisi informasi rahasia dikirim melalui internet, kemudian seseorang menyadap file tersebut tanpa izin dan memanfaatkan informasinya untuk kepentingannya sendiri. Untuk menghindari hal ini, data dapat dibuat menjadi data yang tidak mudah dimengerti bagi penyadap dengan menggunakan teknik enkripsi.

2.3. *Instant Messaging*

Cambridge Advanced Learner's Dictionary (*Instant messaging*, n.d.a) menyebutkan definisi *instant messaging* (IM) adalah jenis layanan yang tersedia di internet yang berfungsi untuk sarana pertukaran pesan teks dengan orang lain yang menggunakan layanan yang sama dalam waktu yang sama. Dictionary.com Unabridged (*Instant messaging*, n.d.b) menyebutkan bahwa *instant messaging* adalah suatu sistem untuk pertukaran pesan elektronik (yang diketik) secara instan melalui internet atau jaringan selular, menggunakan sebuah aplikasi perangkat lunak bersama (*shared software application*) pada komputer personal atau perangkat *mobile*.

Ada banyak protokol yang dapat digunakan untuk layanan *instant messaging*, salah satunya yang populer adalah XMPP. *Extensible Messaging and Presence Protocol* (XMPP) adalah suatu teknologi terbuka yang ditujukan untuk komunikasi waktu nyata (*realtime*), menggunakan XML sebagai format data yang digunakan untuk pertukaran informasi (Andre et al. 2009). XMPP diawali dengan munculnya Jabber pada tahun 1999. Jabber merupakan protokol komunikasi pada jaringan komputer yang sangat populer untuk layanan *instant messaging*. Kemudian Jabber diformalkan oleh IETF (*Internet Engineering Task Force*) pada tahun 2004 menjadi XMPP.

2.4. Enkripsi

Beberapa istilah yang perlu diketahui dalam hal enkrispsi adalah enkripsi (*encryption*), atau dalam tulisan lain disebut juga dengan *encipherment*, adalah proses pembuatan *ciphertext* dari *plaintext*. Proses kebalikannya disebut dekripsi (*decryption*). Algoritma yang menjalankan proses enkripsi dan dekripsi disebut *cipher*. *Plaintext* adalah suatu pesan yang akan dienkripsi. *Ciphertext* adalah pesan yang menyembunyikan *plaintext* di dalamnya. *Key* (kunci) adalah sesuatu yang dibutuhkan oleh *cipher* untuk mengubah *plaintext* menjadi *ciphertext*.

2.5. *Vigenere Cipher*

Vigenere Cipher merupakan algoritma kriptografi klasik yang termasuk ke dalam jenis *polyalphabetic cipher*. *Polyalphabetic cipher* adalah jenis algoritma enkripsi klasik yang tidak melakukan enkripsi per satuan karakter tetapi lebih dari satu karakter. Berbeda dengan *monoalphabetic cipher* yang melakukan enkripsi per satuan karakter.

Key pada *vigenere cipher* merupakan pengulangan dari *key* awal dengan panjang m, dimana $1 \leq m \leq 26$. Maka dapat digambarkan sebagai berikut jika (k1, k2, ..., km) adalah *key* awal. *Plaintext* "Teks ini rahasia" dienkripsi menggunakan *key* "PASCAL". *Key* tersebut dalam angka menjadi (15, 0, 18, 2, 0, 11). P = (T, E, K, S, I, N, I, R, A, H, A, S, I, A) menjadi (19, 4, 10, 18, 8, 13, 8, 17, 0, 7, 0, 18, 8, 0). Maka akan didapatkan C = (8, 4, 2, 20, 8, 24, 23, 17, 18, 9, 0, 3, 23, 0) yang dalam huruf menjadi IECUIYXRSJADXA.

2.6. *Playfair Cipher*

Forouzan (2008) juga menjelaskan tentang *playfair cipher* yang penulis sadur tanpa mengubah makna sebagai berikut. *Secret key* yang digunakan pada algoritma ini terdiri dari 25 huruf alfabet yang disusun dalam matriks 5x5 dengan anggapan huruf I dan J dianggap sama.

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

Gambar 2. Contoh kunci untuk playfair cipher jika hanya menggunakan A-Z

Sebelum dilakukan proses enkripsi, jika dua huruf yang berpasangan adalah huruf yang sama, sebuah huruf (*bogus letter*) disisipkan untuk memisahkan dua huruf tersebut. Setelah menyisipkan *bogus letters*, jika jumlah karakter pada *plaintext* ganjil, maka tambahkan satu *bogus letter* di bagian akhir agar jumlah karakter menjadi genap. *Cipher* ini

menggunakan tiga aturan untuk enkripsi sebagai berikut:

Jika sepasang huruf berada pada baris yang sama pada *secret key*, maka huruf terenkripsi yang sesuai untuk setiap huruf adalah huruf setelahnya ke arah kanan di baris yang sama (dengan kembali memutar ke awal jika huruf *plaintext* merupakan huruf terakhir di dalam baris tersebut).

Jika sepasang huruf berada pada kolom yang sama pada *secret key*, maka huruf terenkripsi yang sesuai untuk setiap huruf adalah huruf di bawahnya pada kolom yang sama (dengan kembali memutar ke awal jika huruf *plaintext* merupakan huruf terakhir di dalam kolom tersebut).

Jika sepasang huruf tidak berada dalam baris dan kolom yang sama pada *secret key*, maka huruf terenkripsi yang sesuai untuk setiap huruf adalah huruf pada baris yang sama namun pada kolom huruf dimana huruf satunya lagi berada

2.6. *Super Encryption*

Super encryption, menurut Ritter (2007), biasanya sebutan untuk proses enkripsi yang terluar pada *multiple encryption*. Ritter (2007) menjelaskan *multiple encryption* adalah melakukan enkripsi pada suatu pesan lebih dari satu kali. Normalnya, melibatkan *key* yang berbeda yang tidak saling terkait untuk masing-masing proses enkripsi dan bisa juga menggunakan *cipher* yang berbeda pula. Tujuan dari dilakukannya *multiple encryption* adalah untuk mengurangi kemungkinan diketahuinya informasi dalam suatu informasi terenkripsi jika *cipher* utamanya telah ada orang lain yang berhasil mengetahui kelemahannya.

3. *End-to-end Encryption*

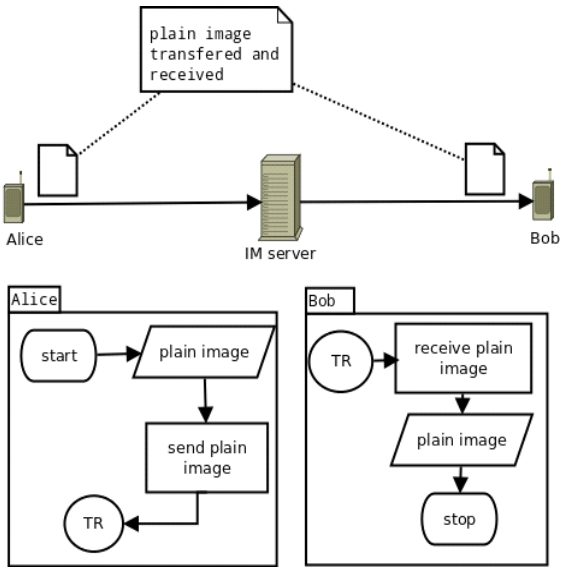
Rouse (2015a) menyatakan *end-to-end encryption* (E2EE) adalah suatu metode untuk mengamankan komunikasi (antara dua orang) dengan mencegah pihak-ketiga dari mengakses data ketika data tersebut di-*transfer* dari titik satu ke titik lainnya. Menurut Andre (2009) *end-to-end encryption* adalah mekanisme enkripsi yang metode enkripsinya dinegosiasikan hanya oleh kedua belah pihak yang akan bertukar pesan sehingga tidak ada pihak lain yang dapat membaca pesan tersebut. Greenberg (2014) juga memberikan penjelasan untuk definisi E2EE yaitu suatu sistem komunikasi dimana orang yang bisa membaca pesannya hanyalah orang yang sedang berkomunikasi tersebut. Tanpa ada orang lain yang dapat mengakses kunci kriptografi yang dibutuhkan untuk mendekripsi percakapan tersebut-begitu juga dengan penyedia layanan komunikasinya tidak dapat mengakses kunci kriptografi yang digunakan.

4. Citra Digital

Menurut Hermawati (2013), citra atau gambar dapat didefinisikan sebagai sebuah fungsi dua dimensi, f(x,y), di mana x dan y adalah koordinat bidang datar, dan harga fungsi f di setiap pasangan koordinat (x,y) disebut intensitas atau level keabuan (*grey level*) dari gambar di titik itu. Jika x,y dan f semuanya berhingga (*finite*), dan nilainya diskrit, maka gambarnya disebut citra digital. Beberapa jenis citra digital yang umum digunakan (Sutoyo et al. 2009), yaitu citra berwarna, citra *grayscale*, dan citra *monochrome*.

III. HASIL DAN PEMBAHASAN

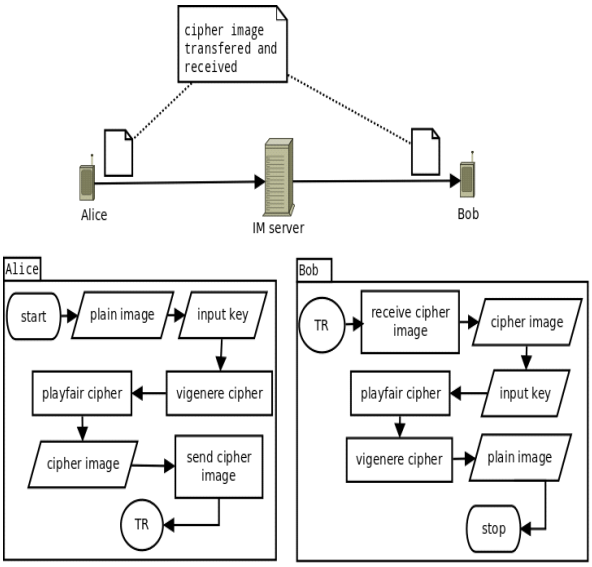
Proses pengiriman citra digital (*file* pada umumnya) pada layanan *instant messaging* tidak menggunakan proses enkripsi. Alur proses pengirimannya dapat dilihat pada gambar berikut.



Gambar 3. Alur pengiriman citra pada layanan IM

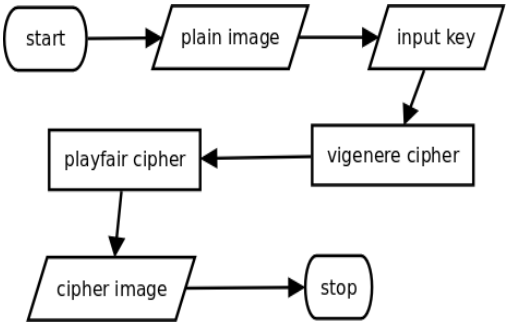
Alur proses pengiriman citra pada aplikasi *mobile instant messaging* yang menggunakan E2EE dalam pengiriman citra

digital yang diusulkan dapat dilihat pada gambar berikut.



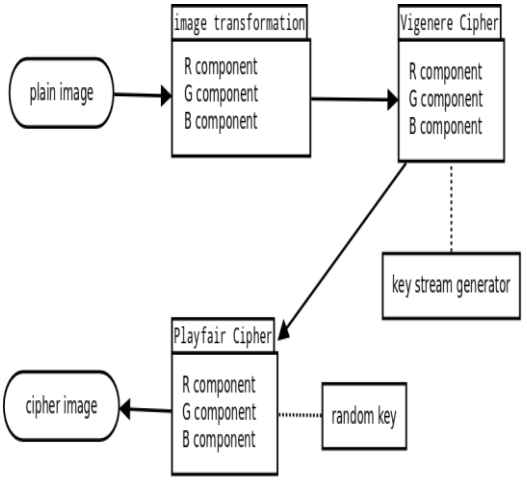
Gambar 4. Alur pengiriman citra dengan enkripsi

Teknik enkripsi yang digunakan adalah *multiple encryption* yang diusulkan oleh Setyaningsih et al. (2012) yaitu penggabungan *vigenere cipher* dengan *playfair cipher* yang terbukti cukup memadai untuk perangkat *mobile*. Alur proses enkripsi citra sebelum dikirim seperti pada gambar di bawah ini. Alur proses dekripsi merupakan kebalikan dari proses enkripsi tersebut.



Gambar 5. Alur proses enkripsi

Sebelum memulai proses enkripsi, kunci yang akan digunakan telah ditentukan. Proses enkripsi dimulai dengan mengurai nilai warna dari setiap *pixel* ke dalam tiga komponen yaitu R (*red*), G (*green*), dan B (*blue*). Nilai-nilai tersebut berupa bilangan bulat positif antara 0 hingga 255. Setelah itu dilakukan enkripsi dengan *vigenere cipher* pada masing-masing nilai komponen warna tersebut. Kemudian dilanjutkan dengan proses enkripsi dengan *playfair cipher*. Proses terakhir adalah penggabungan kembali tiga komponen warna tersebut membentuk *pixel* gambar menjadi gambar yang terenkripsi.



Gambar 6.Proses enkripsi

Kunci yang dibutuhkan dalam proses *multiple encryption* ini adalah kunci untuk *playfair cipher* yang berupa matriks dua dimensi. Kunci ini harus sudah ditentukan sebelum proses enkripsi dan dekripsi dilakukan. Sedangkan kunci yang digunakan pada *vigenere cipher*akan dibuat dari matriks kunci *playfair cipher* dengan menggunakan teknik *keystream generator* (Abhirama 2008).

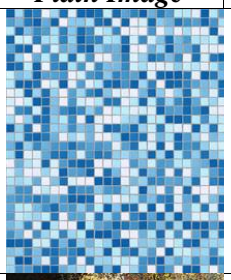
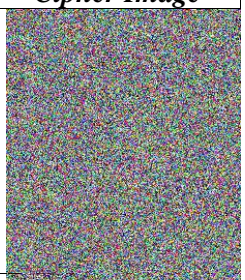
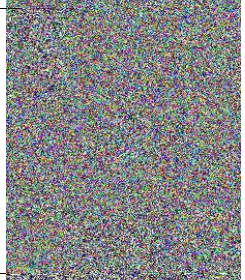
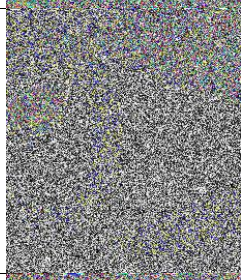
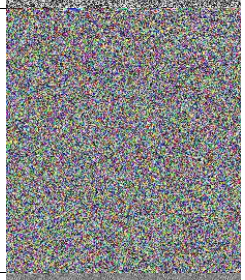
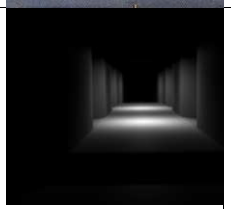
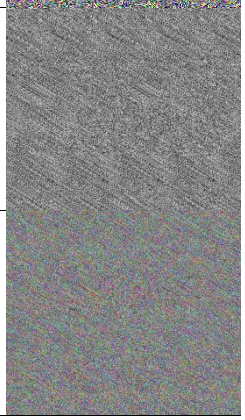
Matriks yang digunakan oleh *playfair cipher* untuk citra digital adalah matriks 16x16. Elemen-elemen matriks ini adalah bilangan bulat dari 0 hingga 255 yang merupakan bilangan representasi warna dari setiap komponen warna RGB.

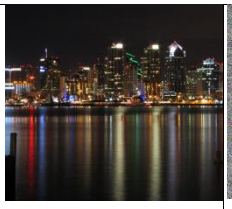
Kunci yang digunakan pada *vigenere cipher* dibuat berdasarkan matriks kunci *playfair cipher* yang telah dibuat sebelumnya. Dengan mengambil n elemen dari matriks kunci (K) dimulai dari elemen pertama (elemen pada posisi 0,0) dengan n = K[0,0]. Umumnya *vigenere cipher*, jika *plaintext* lebih panjang daripada kunci, maka elemen-elemen kunci akan diulang hingga panjang kunci sama dengan panjang *plaintext*. Abhirama (2008) mengusulkan *keystream vigenere cipher* yang tidak lagi menggunakan kunci yang diulang untuk *plaintext* yang panjang. Misal, ki adalah karakter kunci ke-i, dengan i > m, m adalah panjang kunci awal. Karakter kunci ke i didapatkan dengan perhitungan: ki = (ki-1 + ki-m) mod 256.

Setelah melewati tahapan *planning, design*, dan *coding*, beberapa pengujian

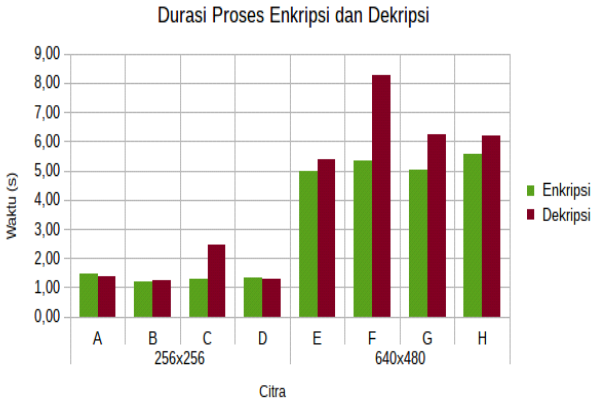
dilakukan pada tahapan terakhir yaitu tahap *testing*. Semua *unit test* dapat dilewati dengan baik, begitu juga dengan *functional test* dan *visual test*. Hasil *visual test* citra asli (*plain image*) dengan citra yang telah dienkripsi (*cipher image*) dapat dilihat pada tabel berikut. Citra no. A – D berdimensi 256x256 dan no. E – G berdimensi 640x480

Tabel 1. Pengujian Citra

#	***Plain Image***	***Cipher Image***
A		
B		
C		
D		
E		
F		

G		
H		

Dari file citra asli, citra hasil enkripsi dan citra hasil dekripsi didapatkan data waktu proses enkripsi/dekripsi yang dapat dilihat pada gambar di bawah ini. Data waktu proses yang ada pada tabel tersebut merupakan waktu proses enkripsi dan dekripsi citra pada perangkat Motorola Moto E.



Gambar 6.Waktu proses enkripsi dan dekripsi

Selisih waktu proses dekripsi dan enkripsi citra dapat dilihat pada grafik pada gambar di atas. Secara umum, selisih waktu proses enkripsi dan dekripsi citra tidak terlalu besar. Namun terdapat perbedaan waktu yang besar pada rata-rata citra berdimensi 256x256 terhadap rata-rata citra berdimensi 640x480. Pada citra berdimensi 256x256, rata-rata waktu proses enkripsi adalah 1,3 detik, sedangkan pada citra berdimensi 640x480 adalah 5,2 detik. Rata-rata keseluruhan waktu proses enkripsi adalah 3,27 detik dan 4,06 detik untuk rata-rata waktu proses dekripsi. Bisa disimpulkan bahwa waktu proses enkripsi relatif sama dengan waktu proses dekripsi dan semakin besar dimensi citra akan

membutuhkan waktu proses enkripsi/dekripsi yang lebih lama.

IV. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat disimpulkan beberapa hal, yaitu:

Hasil *visual test* menunjukkan bahwa dari proses enkripsi dihasilkan *cipher image* yang secara visual tidak lagi sama dengan *plain image* maka bisa dikatakan *plain image* telah tersamarkan. Hasil *visual test* juga menunjukkan bahwa dari semua *plain image* yang berbeda menghasilkan *cipher image* yang memiliki pola yang serupa sehingga hubungan *plain image* dengan *cipher image* sulit diketahui secara visual.

Waktu proses enkripsi relatif sama dengan waktu proses dekripsi dan semakin besar dimensi citra akan membutuhkan waktu proses enkripsi/dekripsi yang lebih lama.Aplikasi yang dibangun telah diuji dengan *unit test* dan *functional test* yang telah dibuat dengan hasil yang menyatakan semua *test* dapat dilewati dengan baik.

Dengan *end-to-end encryption*, proses enkripsi dan dekripsi dilakukan pada masing-masing *device* yang digunakan oleh entitas yang berkomunikasi, sehingga walaupun data *cipher image* yang dikirim dapat diketahui pihak lain (misal: *administrator server* sebagai penyedia layanan), pihak lain tersebut akan sulit untuk mengetahui data *plain image*.

Aplikasi ini merupakan aplikasi XMPP *client* yang dapat digunakan untuk berkomunikasi dengan XMPP *client* lainnya melalui *server* (sebagai penyedia layanan) manapun asalkan menggunakan protokol XMPPHuruf besar hanya ditempatkan pada awal kalimat, kecuali judul naskah, judul bab dan subbab serta symbol. Untuk cuplikan dari jurnal yang berbahasa inggris, dapat tetap ditulis dalam bahasa inggris, dan ditulis dengan *style italic*.

Saran dapat menjadi bahan pertimbangan dalam membangun sistem yang lebih baik di masa yang akan datang diantaranya adalah menerapkan mekanisme pembuatan dan pertukaran kunci yang dapat memudahkan pengguna, meningkatkan kecepatan proses enkripsi dan dekripsi, memberikan beberapa opsi algoritma enkripsi (*cipher*) yang dapat digunakan.

DAFTAR PUSTAKA

[1] Abhirama, Dwitiyo 2008, 'Keystream Vigener Cipher: Modifikasi Vigenere Cipher dengan Pendekatan Keystream Generator', Program Studi Informatika ITB, Bandung.

[2] Andre, Peter Saint, Smith, Kevin, & Troncon, Remco 2009, XMPP: The Definitive Guide, 1st edn, O'reilly, Sebastopol.

[3] Avison, David, & Fitzgerald, Guy 2006, Information Systems Development: Methodologies, Techniques & Tools, 4th edn, McGraw-Hill, New York.

[4] Electronic Frontier Foundation (EFF) 2014, Secure Messaging Scorecard: Which apps and tools actually keep your messages safe?, dilihat pada 4 Maret 2015, <https://www.eff.org/secure-messaging-scorecard>

[5] Forouzan, Behrouz A 2008, Cryptography and Network Security, Int. Edn, McGraw-Hill, New York.

[6] Global Web Index 2014, Mobile Messaging: Functionality and Security are Key Priorities, GWI Trends Q3 2014, dilihat pada 15 April 2015, <https://cdn2.hubspot.net/hub/304927/file-1308893274-pdf/Reports/GWI_Mobile_Messaging_Q3_2014.pdf? t=1419007293428>

[7] Greenberg, Andy 2014, Hacker Lexicon: What is End-to-end Encryption?, dilihat 13 September 2015, <http://www.wired.com/2014/11/hackerlexicon-end-to-end-encryption/>

[8] Hermawati, Fajar Astuti 2013, Pengolahan Citra Digital, Ed. 1, Penerbit Andi, Yogyakarta.

[9] Instant messaging. (n.d.a). Cambridge Advanced Learner's Dictionary and Thesaurus, Cambridge University Press, dilihat 16 September 2015, <http://dictionary.cambridge.org/dictionary/english/instantmessaging>