Perbandingan Algoritma *AES (Advanced Encryption Standard)* dan *3DES(Triple Data Encryption Algorithm)* Menggunakan Manajemen Kunci *ECDH (Elliptic Curve Diffie–Hellman)* Untuk Mengamankan Pesan *Instant Messaging Mobile Android*

Diajukan Sebagai Syarat untuk Menyelesaikan

Pendidikan Program Strata-1 pada

Jurusan Teknik Informatika

Oleh :

MUHAMMAD ANDRI
09021381320031

Jurusan Teknik Informatika

FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2018

LEMBAR PENGESAHAN TUGAS AKHIR

Perbandingan Algoritma *AES (Advanced Encryption Standard)* dan *3DES(Triple Data Encryption Algorithm)* Menggunakan Manajemen Kunci *ECDH (Elliptic Curve Diffie–Hellman)* Untuk Mengamankan Pesan *Instant Messaging Mobile Android*

Oleh :

MUHAMMAD ANDRI
NIM. 09021381320031

Palembang, 27 April 2018

Pembimbing I,

Drs. Megah Mulya, M.T.
NIP. 196602202006041001

Pembimbing II,

Al Farissi, S.Kom., M.Cs.
NIP. 198512152014041001

Mengetahui,
Ketua Jurusan Teknik Informatika

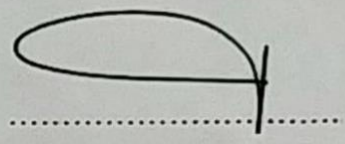
Rifkie Primartha, M.T.
NIP. 197706012009121004

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Jumat tanggal 27 April 2018 telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

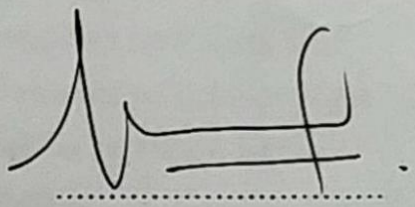
N a m a : Muhammad Andri
Nim : 09021381320031
Judul : Perbandingan Algoritma *AES (Advanced Encryption Standard)* dan *3DES (Triple Data Encryption Algorithm)* Menggunakan Manajemen Kunci *ECDH (Elliptic Curve Diffie–Hellman)* Untuk Mengamankan Pesan *Instant Messaging Mobile Android.*

1. Ketua Penguji



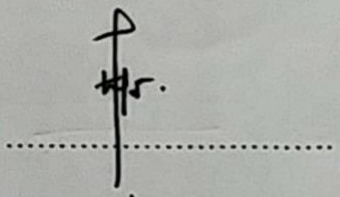
Drs. Megah Mulya, M.T.
NIP. 196602202006041001

2. Sekretaris



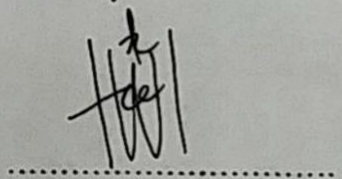
Al Farissi, S.Kom., M.Cs.
NIP. 198512152014041001

3. Penguji I



Yoppy Sazaki,S.Si., M.T
NIP. 197406062015109101

4. Penguji II



Hadipurnawan Satria,Ph.D
NIP. 198004182015109101

Mengetahui,
Ketua Jurusan Teknik Informatika

Rifkie Primartha, ST., M.T.
NIP. 197706012009121004

HALAMAN PERNYATAAN PLAGIAT

Yang bertanda tangan di bawah ini :

Nama	:	Muhammad Andri
NIM	:	09021381320031
Program Studi	:	Teknik Informatika Bilingual
Judul Skripsi	:	Perbandingan Algoritma *AES (Advanced Encryption Standard)* dan *3DES (Triple Data Encryption Algorithm)* Menggunakan Manajemen Kunci *ECDH (Elliptic Curve Diffie–Hellman)* Untuk Mengamankan Pesan *Instant Messaging Mobile Android.*

Hasil Pengecekan Software *iThenticate/Turnitin* : 4 %

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, 27 April 2018

METERAI TEMPEL D665EAFF127127814 6000 ENAM RIBU RUPIAH

(Muhammad Andri)
NIM. 09021381320031

Moto :

- Segala sesuatu dapat terjadi jika Allah SWT menghendakinya.
- Perasaan positif menarik kejadian positif, perasaan negatif menarik kejadian negatif. Jadi tetaplah positif dan hidup dengan ceria.
- You only have one change you know
- Lakukan yang terbaik, hingga kau tak bisa menyalahkan diri sendiri atas semua yang terjadi. (Magdalena Neuner)
- Do what you like and love what you do.
- Let's live a normal life

Kupersembahkan karya tulis ini kepada :

- Allah SWT
- Orang Tua tercinta
- Kedua Pembimbing
- Almamater

Perbandingan Algoritma *AES (Advanced Encryption Standard)* dan *3DES(Triple Data Encryption Algorithm)* Menggunakan Manajemen Kunci *ECDH (Elliptic Curve Diffie–Hellman)* Untuk Mengamankan Pesan *Instant Messaging Mobile Android*.

Oleh :

Muhammad Andri
NIM : 09021381320031

ABSTRAK

Instant messaging merupakan layanan berkomunikasi yang berkembang sangat pesat, perkembangannya ini memerlukan adanya mekanisme keamanan yang dapat menjaga setiap pesan yang dikirim aman dari *eavesdropper*. Penelitian ini akan dilakukan pembangunan aplikasi *instant messaging* yang digunakan untuk membandingkan algoritma AES dan 3DES untuk mengenkripsi pesan, serta menggunakan algoritma ECDH untuk melakukan pertukaran kunci antara pengirim dan penerima. Hasil pengujian kecepatan enkripsi dan dekripsi dari 2 *smartphone* menunjukkan kecepatan *smartphone* yang mendukung *hardware acceleration (AES-NI)* lebih cepat 3—13 kali untuk enkripsi sementara untuk dekripsi 2—10 kali lebih cepat daripada *smartphone* yang tidak mendukung *hardware acceleration (AES-NI)*. Hasil percobaan *delay* tidak menunjukkan perbedaan signifikan diantara kedua *smartphone* bahkan cenderung sama, untuk perbedaan *delay* yang dirasakan antara pengiriman pesan tanpa menggunakan enkripsi dan dekripsi hanya mengalami perbedaan 10—50 ms jika menggunakan algoritma AES dan 3DES dari *library* java JCA. Sementara untuk algoritma *custom* tanpa *library* menunjukkan perbedaan yang sangat signifikan *text* dengan panjang 1024 byte menyebabkan *delay* hingga 6104.4 ms.

Kata Kunci : *Instant Messaging*, Kriptografi, Enkripsi, *Advanced Encryption Standard, Triple Data Encryption Standard, elliptic curve cryptography, Android*

Comparison of AES (Advanced Encryption Standard) and 3DES (Triple Data Encryption Algorithm) Using ECDH (Elliptic Curve Diffie-Hellman Algorithms) Key Management To Secure Messages of Instant Messaging Mobile Android

By :

Muhammad Andri
ID : 09021381320031

ABSTRACT

Instant messaging is a rapidly evolving communications service, this evolution requires a security mechanism that can keep every sent messages safely from eavesdropper (third party or secret listener). In this final project, instant messaging application was developed to compare AES and 3DES algorithms for message encryption, and use ECDH algorithm to perform key exchange between the sender and receiver. The results of testing the speed of encryption and decryption of 2 smartphones show the speed of smartphone that support hardware acceleration *(*AES-NI*)* is 3—13 times faster in encryption, while in decryption is 2—10 times faster than smartphone that do not support hardware acceleration *(*AES-NI*).* The results of delay experiments do not show significant differences between the two smartphones and even tend to be the same, for the difference in the perceived delay between message sending without using encryption and decryption tends to be only 10—50 ms difference if implementing the AES and 3DES algorithm from the java library JCA. While for custom algorithm without library show very significant difference for text with length of 1024 byte causing delay up to 6104.4 ms.

Keywords : *Instant Messaging, Cryptography, Enkripsi, Advanced Encryption Standard, Triple Data Encryption Standard, elliptic curve cryptography, Android*

KATA PENGANTAR

Puji dan syukur kehadirat Allah SWT karena atas rahmat-Nya penulis dapat menyelesaikan tugas akhir ini. Tugas akhir yang berjudul "**Perbandingan Algoritma *AES (Advanced Encryption Standard*) dan *3DES (Triple Data Encryption Algorithm)* Menggunakan Manajemen Kunci *ECDH (Elliptic Curve Diffie–Hellman)* Untuk Mengamankan Pesan *Instant Messaging Mobile Android***" ini disusun untuk memenuhi salah satu persyaratan kelulusan tingkat S1 pada Jurusan Teknik Informatika Universitas Sriwijaya.

Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih yang tak terhingga kepada pihak-pihak telah memberikan dukungan, bimbingan, motivasi dan kemauan kepada penulis untuk menyelesaikan tugas akhir ini, yaitu kepada:

1. Kedua orang tua penulis (ayah dan ibu) yang tidak pernah berhenti untuk selalu memberikan dukungan kepada penulis baik secara materi maupun non-materi.
2. Bapak Jaidan Jauhari, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Rifkie Primartha, ST., M.T. selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya dan penguji.
4. Ibu Anggina Primanita, M.IT selaku Sekretaris Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya dan penguji.
5. Bapak Drs. Megah Mulya, M.T. selaku pembimbing I yang telah sabar membimbing dan membantu penulis.
6. Bapak Al Farissi, S.Kom., M.Cs. selaku pembimbing II yang telah sabar membimbing dan membantu penulis;
7. Bapak dan Ibu Dosen yang selama ini telah melimpahkan ilmunya kepada penulis selama proses belajar mengajar di Fakultas Ilmu Komputer Universitas Sriwijaya.

8. Staf dan karyawan Fakultas Ilmu Komputer atas bantuannya dalam memperlancar kegiatan akademik.
9. Kakak laki-laki saya Iis Apriandi serta seluruh anggota keluarga yang telah memberikan dukungan kepada penulis.
10. Viuty Tiadita yang telah setia memberikan cinta dan dukungan, serta menemani penulis selama masa pengerjaan Tugas Akhir.
11. Teman - teman Teknik Informatika Bilingual angkatan 2013, untuk persahabatan dan masa-masa perkuliahan yang menyenangkan dan tak terlupakan.
12. Untuk semua pihak yang telah membantu penyelesaian tugas akhir ini dan tidak dapat disebutkan satu persatu.

Akhir kata, penulis menyadari bahwa tugas akhir ini jauh dari kata sempurna. Untuk itu penulis mengharapkan kritik dan saran yang membangun dari semua pihak untuk penyempurnaan tugas akhir ini dan semoga tugas akhir ini dapat bermanfaat bagi pihak yang membutuhkan.

Palembang, 27 April 2018

Penulis

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi yang semakin pesat, media komunikasi baru pun banyak bermunculan di kalangan masyarakat. Salah satu media komunikasi yang sedang diminati adalah media komunikasi menggunakan jaringan internet seperti *instant messaging*. *Instant messaging* merupakan suatu bentuk komunikasi yang memungkinkan pengguna untuk mengirimkan pesan singkat ke pengguna lain secara langsung atau *real time*. Beberapa contoh aplikasi *instant messaging* diantaranya *WhatsApp, Line, Hangout, BBM, Telegram*, dan lain sebagainya. Perkembangan *instant messaging* begitu pesat berdasarkan riset yang dilakukan oleh informa pada tahun 2012 menyatakan pengiriman pesan menggunakan *instant messaging* telah mengalahkan pengiriman pesan menggunakan sms dengan perbandingan 19 miliar untuk pengiriman pesan menggunakan *instant messaging* dan 17,6 miliar untuk pengiriman pesan menggunakan sms (David Meyer, 2013).

Berdasarkan perkembangan *instant messaging* maka diperlukan suatu mekanisme pengamanan yang memungkinkan pesan yang dikirim tidak jatuh ke tangan yang tidak berhak. Salah satu cara yang dapat kita lakukan untuk mengamankan pesan adalah dengan memanfaatkan ilmu kriptografi untuk menyamarkan pesan yang dikirim, ke dalam suatu bentuk pesan yang sulit untuk dipahami maknanya. Selain itu diperlukan pengamanan secara *end-to-end (E2E)*

maksudnya pengamanan yang memungkinkan pesan yang dikirim hanya dapat dibaca oleh orang-orang yang sedang berkomunikasi saja, tidak ada *eavesdropper* (pihak ketiga atau *secret listener*) yang dapat mengakses kunci kriptografi yang dibutuhkan untuk mendekripsi percakapan, termasuk penyedia telekomunikasi, penyedia internet bahkan *developer* dari aplikasi *Instant messaging*.

Pengamanan secara *end-to-end (E2E)* hanya mengamankan pesan saat pengiriman serta menutup kemungkinan pesan terbaca oleh pihak ketiga, tetapi ketika pesan tersebut telah sampai dan didekripsi pada sisi *client* pesan pun kembali tidak aman hal ini dikarenakan pesan yang telah didekripsi tersimpan pada *database client*, untuk mengatasi hal ini diperlukan penghapusan automatis terhadap pesan yang dikirim (*self-message-destructing)* dengan menggunakan parameter waktu yang dapat disesuaikan oleh *client* sehingga pesan dapat terhapus sendirinya apa bila parameter waktu telah terpenuhi.

Nugroho dkk, (2015) melakukan penelitian kriptografi dengan menggunakan metode *ECC* (*Elliptic Curve Cryptography)* untuk mengamankan pesan pada aplikasi *instant messaging* dengan cara melakukan penelitian terhadap penyadapan dan pengaruh dari jumlah tambahan waktu *(overhead)* yang digunakan untuk proses enkripsi dan dekripsi. Hasil dari penelitian mereka menunjukan semakin besarnya pesan maka tingkat *overhead* akan semakin tinggi.

Tung *et al*, (2012) melakukan penelitian kriptografi dengan menggunakan metode *RSA (Rivest-Shamir-Adleman)* dan *AES (Advanced Encryption Standard)* untuk mengamankan pengiriman pesan pada *instant messaging* yang memiliki kemampuan untuk menghancurkan pesan sendiri *(Self-Message-Destructing)*.

Hasil dari penelitian mereka menunjukan untuk enkripsi dan dekripsi pesan yang memiliki ukuran dibawah 32 *byte* (1 *byte* = 1 karakter*)* tidak akan berdampak signifikan terhadap kinerja dari aplikasi.

Rihan *et al*, (2015) melakukan penelitian kriptografi untuk membandingkan antara algoritma *AES* dan *DES* yang diimplementasikan dengan menggunakan perangkat keras desktop *Core i5*, dalam penelitiannya dilakukan perbandingan kecepatan enkripsi dan penggunaan cpu dari kedua algoritma. Hasil dari penelitiannya didapatkan algoritma *AES* hanya membutuhkan waktu rata-rata 8.105 detik untuk melakukan enkripsi sedangkan *DES* membutuhkan waktu 22.195 detik untuk data berukuran 15, 30, 45, 60, 75 dan 90 *kilobyte* (1 *kilobyte* = 1000 karakter). Sementara itu untuk penggunaan cpu menunjukkan *AES* memakai setidaknya 4.2% cpu sementara DES hanya 2%.

Dari sejumlah penelitian tentang kriptografi yang telah dijelaskan diatas, maka pada tugas akhir ini akan membandingkan antara metode Algoritma *AES (Advanced Encryption Standard)* dan 3*DES (Triple Data Encryption Algorithm)* yang akan digunakan untuk enkripsi dan dekripsi dari pesan *instant messaging*, kedua algoritma ini berjenis *symmetric block cipher* yang memiliki kelebihan dalam hal enkripsi dan dekripsi data berukuran besar relatif lebih cepat jika dibandingkan dengan algoritma kriptografi *Asymmetric* lain.

Pemilihan algoritma *3DES* didasarkan pada publikasi dari *NIST (National Institute of Standards and Technology)* dalam dokumen 800-67, sebagai badan yang mempublikasikan algoritma *DES* yang mengatakan jika algoritma *DES* sudah tidak direkomendasikan lagi dan disarankan untuk mengganti menjadi *3DES*. Selain itu

perlu diketahui mana algoritma yang lebih unggul jika diimplementasikan pada perangkat lunak *mobile android*, tidak seperti perangkat desktop berbasis intel atau amd yang menggunakan arsitektur x86 perangkat *mobile android* kebanyakan berbasis *ARM* yang belum mendukung *hardware acceleration* untuk *AES (AES-NI)*. Sehingga penelitian ini akan memfokuskan untuk mengetahui kecepatan enkripsi dan dekripsi, serta ukuran *cipher text* jika dibandingkan dengan *plain text* dari kedua algoritma yang akan diimplementasikan pada perangkat *mobile android* berbasis *ARM*. Selain itu juga akan digunakan algoritma *ECDH (Elliptic Curve Diffie-Hellman)* yang merupakan turunan dari algoritma *ECC* (*Elliptic Curve Cryptography)* sebagai manajemen kunci sehingga memungkinkan pengguna *instant messaging* tidak perlu lagi untuk menukar kunci mereka secara manual.

1.2 Perumusan Masalah

Permasalahan dari penelitian ini adalah bagaimana perbandingan algoritma *AES* dan 3*DES* menggunakan manajemen kunci algoritma *ECDH (Elliptic Curve Diffie-Hellman)* yang akan dibangun pada perangkat *mobile smartphone* berbasis *ARM* yang tidak memiliki *feature Hardware Accelaration (AES-NI)* dan yang telah memiliki *feature Hardware Accelaration (AES-NI)* untuk algoritma kriptografi.

1.3 Tujuan dan Manfaat Penelitian

1.3.1 Tujuan Penelitian

Tujuan penelitian ini adalah membuat suatu aplikasi *Instant messaging* untuk membandingkan algoritma *AES* dan 3*DES* dengan menggunakan manajemen kunci *ECDH (Elliptic Curve Diffie-Hellman)* untuk mengetahui perbedaan kecepatan enkripsi dan dekripsi. Serta untuk mengetahui perbedaan waktu *(delay)*

yang dirasakan oleh pengguna ketika pesan dikirim oleh pengirim hingga pesan sampai ke penerima.

1.3.2 Manfaat Penelitian

Manfaat penelitian ini yaitu menghasilkan perangkat lunak *Instant messaging* yang dapat melakukan enkripsi dan dekripsi pesan sehingga diharapkan pesan yang dikirim melalui aplikasi *Instant messaging* ini aman dari seseorang yang mencoba untuk menyusup ke dalam percakapan yang dilakukan pengguna. Serta untuk mengetahui perbedaan dari algoritma *AES* dan 3*DES* yang akan diterapkan pada perangkat *mobile android*.

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini diantaranya:

1. Aplikasi yang dibuat hanya dapat dijalankan pada sistem operasi android (Minimal Android Versi 5.1).
2. Aplikasi *instant messaging* bersifat *client server* dengan menggunakan *realtime database*.
3. Pengamanan hanya digunakan untuk mengamankan pesan berupa teks dan *emoticon* berbasis *unicode.*
4. Enkripsi hanya diterapkan pada *one-to-one chat* saja bukan *group chat.*
5. Panjang teks yang akan dilakukan pengujian yaitu sebesar 64, 128, 254, 512, 1024 *byte* (1 *byte* = 1 karakter).
6. Algoritma yang digunakan adalah *AES 128-bit*, *3DES 168-bit*, dan *ECDH 256-bit (secp256r1).*

7. Proses pengujian menggunakan koneksi yang dibatasi untuk download 2 Mbps dan upload 2 Mbps.
8. Proses pengujian delay menggunakan waktu dari server *network time protocol (NTP)* dari time.google.com.
9. Percobaan enkripsi dan dekripsi dalam keadaan kedua smartphone hanya membuka aplikasi MeChat, tidak ada aplikasi lain yang berjalan pada *recent app* dan *backgroud*, untuk aplikasi yang berjalan pada *backgroud* hanya aplikasi default dari google seperti *google services* dan beberapa aplikasi *default* produsen *smartphone*. Sementara itu aplikasi seperti facebook, whatsapp, path dll tidak dalam keadaan tidak terinstal.

1.5 Metode Penelitian

Langkah-langkah yang dilakukan dalam tugas akhir ini antara lain :

1. Mempelajari dan mengkaji semua konsep terkait dengan kriptografi khususnya mengenai konsep *AES (Advanced Encryption Standard)*, *3DES (Triple Data Encryption Algorithm),* dan *ECC (Elliptic Curve Cryptography)* yang akan akan diimplementasikan pada perangkat lunak.
2. Mengumpulkan informasi mengenai data *chat* yang sering dikirim oleh pengguna seperti panjang karakter *chat*, *emoticon*, dan spesial karakter yang sering digunakan.
3. Melakukan pengembangan perangkat lunak dengan menggunakan *RUP* (*Rational Unified Process*).

4. Melakukan proses pertukaran kunci menggunakan algoritma *ECDH (Elliptic Curve Diffie-Hellman)* untuk mendapatkan kunci rahasia (shared key) yang akan digunakan oleh pengirim dan penerima.
5. Melakukan proses enkripsi maupun dekripsi pada data yang hendak dikirim menggunakan algoritma *AES (Advanced Encryption Standard)* atau *3DES (Triple Data Encryption Algorithm).*
6. Melakukan analisis terhadap hasil pemakaian perangkat lunak, membahas hasil analisis terhadap perangkat lunak yang telah dibangun, membuat kesimpulan, dan menyempurnakan laporan.

1.6 Metode Pengembangan Perangkat Lunak

Metode pengembangan perangkat lunak yang digunakan dalam penelitian ini adalah *Rational Unified Process* (RUP) yang merupakan salah satu model pengembangan perangkat lunak berorientasi objek yang bersifat *iterative incremental*. Langkah-langkah yang akan dilakukan dalam penelitian ini akan dijelaskan pada Tabel I-1 berikut ini :

Tabel I-1. Kegiatan Pengembangan Perangkat Lunak Berdasarkan RUP

	Insepsi	Elaborasi	Konstruksi	Transisi
Pemodelan Bisnis	a. Menganalisis deskripsi umum system. b. Menentukan aktor yang terlibat yaitu pengguna aplikasi *instant messaging*. c. Membuat model *use case.*	a. Membuat diagram *use case* berdasarkan *use case* yang telah dimodelkan pada tahap insepsi. b. Membuat skenario *use case* utama yang menggambarkan urutan interaksi aktor terhadap sistem.	a. Membuat aktor *use case* dengan Microsoft Visio 2016. b. Membuat skenario yang berisi urutan interaksi aktor menggunakan Microsoft Word 2016.	a. Menguji *use case* serta skenario apakah telah sesuai dengan kebutuhan sistem kepada aktor. b. Membuat dokumentasi *use case* dan skenario dalam bentuk laporan.
Kebutuhan Perangkat Lunak	a. Melakukan pencarian jurnal-jurnal yang berhubungan dengan Kriptografi khususnya	a. Menganalisa kebutuhan perangkat lunak. b. Menganalisa resiko yang akan ditemui saat		a. Mendokumentasikan kebutuhan perangkat lunak yang digunakan dalam bentuk laporan.

	yang berhubungan dengan *ECC, AES dan 3DES* sebagai referensi/rujukan. b. Menggunakan *android studio* untuk mengimplementasikan *ECC, AES dan 3DES* pada *instant messaging*. c. Menyiapkan perangkat keras yang digunakan yaitu *Processor* Intel® Core™ i7-2600K Quad Core @ 3.80 GHz, RAM 8.00 GB, *Hard Disk* 1 TB,	pembangunan perangkat lunak.		

	NVIDIA GTX 660 TI. d. Menyiapkan perangkat keras yaitu *smartphone* android Meizu MX4 Pro dengan *chipset* Exynos 5430 Octa, RAM 3.00 GB, *Internal Memori* 32GB dan *GPU* Mali-T628MP6			
Analisis dan Desain	a. Mendesain tampilan awal *prototype* perangkat lunak	a. Mendesain model kelas analisis, diagram kelas, dan *sequence diagram* dari perangkat lunak.	a. Membuat kelas analisis, kelas diagram dan *sequence diagram* menggunakan Microsoft Visio 2013.	a. Membuat kelas analisis, kelas diagram dan *sequence diagram*

				dalam bentuk laporan
Implementasi	a. Bahasa pemprograman yang digunakan dalam membuat sistem ini adalah bahasa Java.	a. Melakukan revisi prototype antarmuka menggunakan Microsoft Visio 2013. b. Mengidentifikasi rancangan antar muka.	a. Mengimplementasikan hasil analisis dan desain kebutuhan ke dalam *coding* program.	a. Melakukan penyempurnaan pemprograman sampai pada tahap akhir.
Pengujian	a. Melakukan perencanaan pengujian terhadap sistem berupa data-	a. Pengujian menggunakan masukan data berupa teks disertai dengan beberapa spesial karakter dan *emoticon*.	a. Melakukan penelitian tingkat lanjut dengan melihat keefektikan penggunaan *AES dan*	a. Membuat dokumentasi terhadap evaluasi pengujian terkait dengan keberhasilan

	data yang akan diujikan nanti.	b. Melakukan pengujian terhadap perangkat lunak berdasarkan kebutuhan yang telah dirancang	*3DES menggunakan kunci ECDH*. b. Melakukan perbaikan perangkat lunak apabila terdapat kesalahan berdasarkan hasil pengujian.	enkripsi dan dekripsi data. b. Membuat kesimpulan

1.6.1 Jenis Data

Jenis data yang digunakan dalam penelitian ini adalah data primer yang dikumpulkan dari hasil *chat* yang sering dikirim oleh pengguna dan dari beberapa jurnal yang membahas mengenai kriptografi pada aplikasi *instant messaging*.

1.6.2 Sumber Data

Sumber data yang digunakan dalam penelitian ini berasal dari jurnal, artikel, berita, atau pun chat yang sering dikirim oleh pengguna aplikasi *instant messaging*.

1.6.3 Pengumpulan Data

Teknik pengumpulan data yang digunakan pada tugas akhir ini adalah:

1. Mengumpulkan Secara Langsung

   Data yang digunakan dalam penelitian ini adalah data berupa teks percakapan yang dikirimkan oleh seorang user *(sender)* kepada user lain *(receiver)* pada aplikasi *instant messaging.* Data sample teks yang digunakan terdiri dari beberapa teks dengan panjang teks yang berbeda dan terdiri dari kombinasi huruf, angka, spesial karakter maupun *emoticon* berbasis *unicode*.

2. Studi Kepustakaan

   Studi kepustakaan (*literature*) digunakan untuk mencari referensi atas pustaka-pustaka yang dijadikan acuan dalam penelitian, seperti jurnal, artikel, buku-buku, prosiding, dan karya ilmiah lainnya. Adapun pustaka yang menjadi acuan adalah yang membahas tentang kriptografi.

1.7 Sistematika Penulisan

Dalam penulisan tugas akhir ini, sistematika penulisan adalah sebagai berikut :

BAB I. PENDAHULUAN

Meliputi latar belakang, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah/ruang lingkup, metodologi penelitian, dan sistematika penulisan.

BAB II. LANDASAN TEORI

Pada bab ini akan dibahas dasar-dasar teori yang digunakan dalam penelitian, seperti algoritma AES (*Advanced Encryption Standard), 3DES (Triple Data Encryption Standard*), *Firebase,* dan metode pengembangan perangkat lunak *Rational Unified Process*.

BAB III. ANALISA DAN PERANCANGAN

Pada bab ini akan dibahas mengenai analisis sistem yang berjalan, pernyataan kebutuhan, *use case*, *domain model*, *sequence diagram,* dan *class diagram*.

BAB IV. IMPLEMENTASI DAN PENGUJIAN

Pada bab ini akan dibahas mengenai lingkungan implementasi sistem pengenalan suara, hasil eksekusi, dan hasil pengujian.

BAB V. KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dari semua uraian-uraian pada bab-bab sebelumnya dan juga berisi saran-saran yang diharapkan berguna dalam penerapan sistem ini.

DAFTAR PUSTAKA

Tung, T.-Y., Lin, L., & Lee, D. T. 2012. *Pandora Messaging: An Enhanced Self Message-Destructing Secure Instant*. Internasional Conference on Advanced Information Networking and ApplicationsWorkshops.

Nugroho, Andreas, dan Munir, Rinaldi. 2015. Aplikasi Enkripsi Instant Messaging Pada Perangkat Mobile Dengan Menggunakan Algoritma *Elliptic Curve Cryptography (ECC)*. Kampus institut teknologi bandung

Nugroho, Andreas, dan Munir, Rinaldi. 2015. *A Performance Comparison of Encryption Algorithms AES and DES. International Journal of Engineering Research & Technology (IJERT),* Vol. 8, Issue 12.

Kruchten, P. 2001. *THE RATIONAL UNIFIED PROCESS: AN INTRODUCTION*. Addison-Wesley.

Meyer, D. 2013. *Chat apps have overtaken SMS by message volume, but how big a disaster is that for carriers?*. Diambil dari Gigaom: https://gigaom.com/2013/04/29/chat-apps-have-overtaken-sms- by-message-volume/, Tanggal akses : 15 Desember 2016.

Federal Information Processing Standards Publications. 1999. FIPS PUB 46-3. Data Encryption Standard (DES). Diambil Dari Nist: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf. Tanggal akses : 10 Agustus 2016.

Federal Information Processing Standards Publications. 2012. FIPS PUB 800-67. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. Diambil Dari Nist:

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-67r1.pdf. Tanggal akses : 12 Januari 2017.

Federal Information Processing Standards Publications. 2001. FIPS PUB 197. Advanced Encryption Standard (AES). Diambil Dari Nist: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf. Tanggal akses : 9 Juli 2016.

Knudsen, Jonathan B. 2001. *Java Cryptography*. New York : O'Reilly Media.