SISTEM PENGAMANAN PESAN MENGGUNAKAN KRIPTOGRAFI AES DAN DIGITAL SIGNATURE RSA-MD5 BERBASIS MOBILE

Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika

Oleh:

Ahmad Emir Alfatah
09021381722130

JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2021

LEMBAR PENGESAHAN TUGAS AKHIR

SISTEM PENGAMANAN PESAN MENGGUNAKAN KRIPTOGRAFI AES DAN DIGITAL SIGNATURE RSA-MD5 BERBASIS MOBILE

Oleh:

AHMAD EMIR ALFATAH
NIM : 09021381722130

Palembang, 25 Agustus 2021

Pembimbing I,	Pembimbing II,
Julian Supardi, M.T	Mastura Diana Marieska, M.T
NIP. 197207102010121001	NIP. 198603212018032001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP 197812222006042003

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Selasa tanggal 3 Agustus 2021 telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama	:	Ahmad Emir Alfatah
NIM	:	09021381722130
Judul	:	Sistem Pengamanan Pesan Menggunakan Kriptografi AES dan Digital Signature RSA-MD5 Berbasis Mobile

1. Pembimbing I

   Julian Supardi, M.T. .....
   NIP. 197207102010121001

2. Pembimbing II

   Mastura Diana Marieska, M.T. .....
   NIP. 198603212018032001

3. Penguji I

   Dr. Abdiansah, S.Kom., M.Cs. .....
   NIP. 198410012009121005

4. Penguji II

   Osvari Arsalan, M.T. .....
   NIP. 198806282018031001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Ahmad Emir Alfatah
NIM	: 09021381722130
Program Studi	: Teknik Informatika Bilingual
Judul Skripsi	: Sistem Pengamanan Pesan Menggunakan Kriptografi AES dan Digital Signature Berbasis Mobile
Hasil Pengecekan Software *iThenticate/Turnitin*	: **8 %**

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, 25 Agustus 2021

(Ahmad Emir Alfatah)

NIM. 09021381722130

MOTTO DAN PERSEMBAHAN

“God’s timing is always perfect. Trust His delays. He’s got you”

-Tony Evans-

“Kamehameha”

-Raditya Dika-

Kupersembahkan karya tulis ini kepada:

- Kedua orang tua dan keluargaku
- Sahabat dan Teman Seperjuanganku
- Fakultas Ilmu Komputer
- Universitas Sriwijaya

Mobile-Based Message Security System Using AES Cryptography and Digital Signature RSA-MD5

By:
Ahmad Emir Alfatah
09021381722130

ABSTRACT

A chat message has high privacy and there are still many chat applications that do not provide security so the messages can be intercepted and known by unwanted people. AES cryptography has generally been implemented in most chat messenger applications. However, with cases of eavesdropping and fraud still rampant, it is necessary to improve message security schemes that can strengthen the security and the authenticity of messages. This study aims to combine AES cryptography and digital signature in securing mobile-based chat messengers so the scheme can secure messages in terms of security and authenticity of text messages. This study uses text consisting of 10 to 100 message characters. From the results of the tests, it can be concluded that AES cryptography and digital signature is considered good for securing text messages because the Avalanche Effect value is following the Strict Avalanche Effect standard. With the addition of a digital signature method, it can improve message security for the better because the authenticity of the message can be guaranteed with an insignificant increase time compared to using only AES cryptography with the average time required for the security process using AES cryptography is 6.71 ms and 6.54 ms, while the average time required for the security process with the addition of the digital signature method is 7.54 ms and 7.19 ms.

Keyword: AES, Digital Signature, Avalanche Effect, Chat Messenger, Android

Sistem Pengamanan Pesan Menggunakan Kriptografi AES dan Digital Signature RSA-MD5 Berbasis Mobile

Oleh:
Ahmad Emir Alfatah
09021381722130

ABSTRAK

Suatu pesan *chat* memiliki privasi yang tinggi dan masih banyak aplikasi *chat* tidak menyediakan keamanan sehingga pesan dapat disadap dan diketahui oleh orang yang tidak diinginkan. Kriptografi AES umumnya telah diterapkan pada kebanyakan aplikasi *chat messenger* tetapi dengan masih maraknya kasus penyadapan dan penipuan maka diperlukan suatu skema pengamanan yang dapat meningkatkan keamanan dan keaslian pada pesan. Penelitian ini bertujuan untuk menggabungkan skema kriptografi AES dan *digital signature* dalam mengamankan pesan *chat messenger* berbasis mobile sehingga dapat mengamankan pesan dari segi keamanan dan keaslian pesan teks. Penelitian ini menggunakan teks yang terdiri dari 10 hingga 100 karakter pesan. Dari hasil pengujian dapat disimpulkan bahwa kriptografi AES dan *digital signature* dinilai baik untuk mengamankan pesan dikarenakan nilai *Avalanche Effect* yang sesuai dengan standar Strict Avalanche Effect dan penambahan metode *digital signature* juga dapat meningkatkan keamanan pesan menjadi lebih baik karena pesan dapat terjamin keasliannya dengan penambahan waktu yang tidak signifikan dibandingkan dengan hanya menggunakan kriptografi AES dengan rata-rata waktu yang dibutuhkan pada proses pengamanan menggunakan kriptografi AES adalah 6.71 ms dan 6.54 ms, sedangkan rata-rata waktu yang dibutuhkan pada proses pengamanan dengan penambahan metode digital signature adalah 7.54 ms dan 7.19 ms.

Kata Kunci: AES, Digital Signature, Avalanche Effect, Chat Messenger, Android

KATA PENGANTAR

Penulis ucapkan puji syukur kepada Allah atas berkat dan rahmat-Nya yang telah diberikan kepada Penulis sehingga dapat menyelesaikan Tugas Akhir dengan judul "**Sistem Pengamanan Pesan Menggunakan Kriptografi AES dan Digital Signature RSA-MD5 Berbasis Mobile**" dengan baik untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Pada kesempatan ini, penulis ingin mengucapkan terima kasih kepada pihak-pihak yang telah berperan memberikan bantuan dan dukungan baik secara langsung maupun secara tidak langsung dalam menyelesaikan tugas akhir ini.

Penulis ingin menyampaikan rasa terima kasih kepada:

1. Kedua orang tuaku, Joko Yuliyanto dan Heindriyati yang selalu mendoakan serta memberikan dukungan baik moril maupun materil.
2. Bapak Jaidan Jauhari, M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya beserta jajarannya. Ibu Alvi Syahrini Utami, M.Kom. selaku Ketua Jurusan Teknik Informatika beserta jajarannya, dan Ibu Mastura Diana Marieska, M.T. selaku Sekretaris Jurusan Teknik Informatika.
3. Bapak Drs. Megah Mulya, M.T. (Alm) selaku dosen pembimbing saya yang telah membimbing dan mengarahkan saya sehingga saya dapat mengawali tugas akhir saya dengan baik.
4. Bapak Julian Supardi, M.T. selaku dosen pembimbing I dan Ibu Mastura Diana Marieska, M.T. selaku pembimbing II yang telah membimbing, mengarahkan, dan memberikan motivasi penulis dalam proses perkuliahan dan pengerjaan Tugas Akhir.
5. Ibu Desty, selaku dosen pembimbing akademik yang telah membimbing, mengarahkan dan memberikan motivasi penulis dalam proses perkuliahan.
6. Bapak Dr. Abdiansah, S.Kom., M.Cs. selaku dosen penguji I, dan Bapak Osvari Arsalan, M.T. selaku dosen penguji II yang telah memberikan saran dan masukan dalam pengerjaan Tugas Akhir saya sehingga dapat menjadi lebih baik.

7. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Mbak Wiwin, selaku staff administrasi Teknik Informatika Bilingual, dan seluruh staff Fakultas Ilmu Komputer Universitas Sriwijaya yang telah membantu dalam kelancaran proses administrasi dan akademik selama masa perkuliahan.
9. Jessica Julia, Ridha Ayu, dan Aldi Ariqi yang selalu memberikan support dari awal hingga akhir dan dalam keadaan apapun. Teman jurusan Teknik Informatika yang telah membantu selama masa perkuliahan, maaf tidak dapat disebutkan satu persatu.
10. Seluruh pihak yang telah membantu dalam penyusunan dan penyempurnaan tugas akhir ini yang tidak dapat disebutkan satu persatu.

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan disebabkan keterbatasan pengetahuan dan pengalaman, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk kemajuan penelitian selanjutnya. Akhir kata semoga Tugas Akhir ini dapat berguna dan bermanfaat bagi kita semua.

Palembang, 25 Agustus 2021

Ahmad Emir Alfatah

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab pendahuluan ini akan membahas mengenai latar belakang diambilnya topik “Sistem Pengamanan Pesan Menggunakan Kriptografi AES dan Digital Signature RSA-MD5 Berbasis Mobile”. Pada bab ini juga membahas rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika penulisan, dan gambaran umum dari keseluruhan kegiatan yang dilakukan dalam penelitian.

1.2 Latar Belakang

Pada perkembangan teknologi informasi yang pesat saat ini, *smartphone* telah menjadi bagian yang sangat penting di kehidupan sehari-hari. Hal ini dapat dibuktikan dengan seringnya penggunaan *smartphone* dalam mencari informasi, mengirim pesan pada aplikasi *chat messenger*, bermain *game* dan lain-lain (Ali & Sagheer, 2017). Aplikasi pesan obrolan atau *chat messenger* merupakan perangkat lunak yang dapat mengirimkan pesan secara *real time* ke banyak *device*. Suatu pesan *chat* memiliki privasi yang tinggi, saat ini masih banyak aplikasi *chat* tidak menyediakan keamanan pada pesan sehingga pesan dapat disadap dan diketahui oleh orang yang tidak diinginkan. Beberapa aplikasi chat yang memiliki fitur keamanan pun belum tentu memiliki keamanan yang baik dalam menjaga privasi user. Untuk mencegah masalah tersebut diperlukan sistem keamanan yang dapat meningkatkan keamanan pesan yaitu kriptografi. (Suryanto et al., 2017).

Kriptografi memiliki banyak metode algoritma salah satunya adalah Advance Encryption Standard (AES). AES mempunyai ukuran blok sebesar 128, 192, 256 bit dengan panjang *key* yang berbeda-beda. Pada proses enkripsi dan dekripsi, proses AES sangat bergantung dengan panjangnya kunci, semakin panjang kunci maka proses enkripsi dan dekripsi akan memakan waktu lebih lama. Algoritma kriptografi AES memiliki performa lebih lambat dari pada algoritma *block chiper* lain tetapi AES mempunyai keamanan yang paling baik (Putri et al., 2018).

Pada penelitian tentang sistem pengamanan pesan yang pernah dilakukan, pengembangan aplikasi *chat messenger* dengan judul "Design of an Android Application for Secure Chatting" telah menerapkan sistem keamanan Kriptografi AES pada aplikasi *chat messenger*, tetapi belum menerapkan Digital Signature pada metode pengamanan pesan yang dibuatnya (Ali & Sagheer, 2017). Digital Signature dapat mengamankan pesan yang dikirim oleh seseorang dengan fungsi *hash* sehingga dapat menjaga keutuhan dan integritas pesan dengan membangkitkan *message digest* pada pesan. Jika terjadi perbedaan antara pesan dan *message digest* pesan, maka dapat disimpulkan adanya perubahan pada pesan. Sehingga dengan penggunaan Digital Signature ini dapat dipastikan keasliannya dan dapat mencegah penerimaan pesan dari orang yang tidak diinginkan (Pairin, 2018).

1.3 Rumusan Masalah

Berdasarkan latar belakang diatas, fokus permasalahan yang akan dibahas pada penelitian ini adalah bagaimana cara menjaga kerahasiaan pesan dan menjamin keaslian pesan dengan mengimplementasikan skema penggabungan algoritma kriptografi AES dan *digital signature* menggunakan RSA dan MD5 pada aplikasi *chat messenger* berbasis Mobile.

1.4 Tujuan Penelitian

Berikut adalah tujuan penelitian ini:

1. Mengembangkan perangkat lunak yang mengimplementasikan sistem pengamanan pesan dan penjaminan keaslian pesan dengan algoritma kriptografi AES dan *digital signature* menggunakan RSA dan MD5 pada aplikasi *chat messenger* berbasis Mobile.
2. Melakukan pengukuran kualitas kekuatan dan tingkat keamanan pesan yang diamankan dengan Kriptografi AES menggunakan Avalanche Effect.
3. Melakukan pengukuran kecepatan waktu komputasi pada proses pengamanan pesan dengan algoritma kriptografi AES dan *digital signature* menggunakan RSA dan MD5 berdasarkan waktu proses.

1.5 Manfaat Penelitian

Berikut adalah manfaat penelitian ini:

1. Menghasilkan aplikasi *chat messenger* dengan menerapkan metode pengamanan pesan kriptografi AES & Digital Signature.
2. Mengetahui seberapa baik skema pengamanan pesan menggunakan kriptografi AES & Digital Signature untuk mengamankan dan menjaga keaslian pesan user pada aplikasi *chat messenger* berbasis Android.
3. Menjaga dan menjamin keamanan dan keaslian pesan menggunakan kriptografi AES dan Digital Signature berbasis Android.
4. Dapat digunakan sebagai referensi bagi peneliti di bidang kriptografi.

1.6 Batasan Masalah

Batasan masalah dalam penelitian ini adalah:

1. Ukuran blok pada algoritma kriptografi Advance Encryption Standard yang digunakan adalah 128 bit dan ukuran *key* yang digunakan adalah 32 karakter untuk hexadecimal dan 24 karakter untuk base64.
2. Metode kriptografi dan *hash* yang digunakan pada Digital signature adalah RSA dan MD5.
3. Skenario Avalanche Effect hanya dilakukan pada perubahan 1 karakter pesan.
4. Pengamanan pesan hanya dilakukan pada pesan teks dan dari sisi serangan *Men in The Middle*.

1.7 Sistematika Penulisan

Penulis dalam menulis laporan penelitian ini mengikuti sistematika penulisan skripsi Fakultas Ilmu Komputer Universitas Sriwijaya yang terdiri dari beberapa bab yaitu:

BAB I. PENDAHULUAN

Bab ini membahas latar belakang penelitian, rumusan masalah penelitian, tujuan penelitian, manfaat penelitian, batasan masalah penelitian serta sistematika penulisan pada penelitian ini.

BAB II. KAJIAN LITERATUR

Bab ini membahas landasan teori yang digunakan pada penelitian tugas akhir.

BAB III. METODELOGI PENELITIAN

Bab ini membahas tahapan yang dilakukan pada penelitian tugas akhir. Perencanaan tahapan penelitian dijelaskan dengan kerangka kerja dan manajemen proyek penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Bab ini membahas tahapan yang dilakukan dalam proses pengembangan perangkat lunak sistem keamanan pesan menggunakan kriptografi AES dan *digital signature* berbasis *mobile*.

BAB V. HASIL DAN ANALISIS PENELITIAN

Bab ini akan membahas mengenai hasil dari pengembangan perangkat lunak. Hasil analisis digunakan sebagai kesimpulan yang dapat diambil dari penelitian ini.

BAB VI. KESIMPULAN DAN SARAN

Bab ini akan membahas mengenai kesimpulan dari bab sebelumnya dan saran yang dapat berguna dari penelitian ini.

1.8 Kesimpulan

Bab ini telah membahas latar belakang pada penelitian ini yaitu penerapan serta analisa kualitas kekuatan dan kecepatan pengamanan pesan pada aplikasi *chat messenger* berbasis Android menggunakan algoritma kriptografi Advance Encryption Standard dan Digital Signature.

DAFTAR PUSTAKA

Abraham, F. Z., Santosa, P. I., & Winarno, W. W. (2018). Tandatangan Digital Sebagai Solusi Teknologi Informasi Dan Komunikasi (Tik) Hijau: Sebuah Kajian Literatur (Digital Signature As Green Information and Communication Technology (Ict) Solution: a Review Paper). *Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, *9*(2), 111. https://doi.org/10.17933/mti.v9i2.120

Ali, A., & Sagheer, A. (2017). Design of an Android Application for Secure Chatting. *International Journal of Computer Network and Information Security*, *9*, 29–35. https://doi.org/10.5815/ijcnis.2017.02.04

Arief, A. (2016). Implementasi Kriptografi Kunci Publik dengan Algoritma RSA CRT pada Aplikasi Instant Messaging. 3(1): 46–54.

Budi K. Hutasuhut., Syahril Efendi., & Zakarias Situmorang. (2019). Digital Signature untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA. Jurnal Nasional Informatika dan Teknologi Jaringan. DOI: https://doi.org/10.30743/infotekjar.v3i2.1019

Jayant P Bhoge., & Dr. Prashant N. Chatur. (2014). Avalanche Effect of AES Algorithm. International Journal of Computer Science and Information Technologies, 5(3), 3101-3103

Pairin, Y. Bin. (2018). Kode Autentikasi Hash pada Pesan Teks Berbasis Android. Eksplora Informatika, 8(1), 6. https://doi.org/10.30864/eksplora.v8i1.129

Putri, G. G., Setyorini, W., & Rahayani, R. D. (2018). Analisis Kriptografi Simetris AES dan Kriptografi Asimetris RSA pada Enkripsi Citra Digital. *ETHOS (Jurnal Penelitian Dan Pengabdian)*, *6*(2), 197–207. https://doi.org/10.29313/ethos.v6i2.2909

Sardju, E.R., Magdalena, R. & Atmaja, R.D. 2015. Implementasi Algoritma Rsa Untuk Enkripsi Dan Dekripsi Sms (short Message Service) Pada Ponsel Berbasis Android. eProceedings of Engineering, 2(2): 2435–2442.

Suryanto, I., Suhery, C., & Brianorman, Y. (2017). Pengembangan Aplikasi Chat Messenger dengan Metode Advanced Encryption Standard (AES) pada Smartphone. Jurnal Coding Sistem Komputer Untan, 03(2), 1–10.

Siregar, K. (2019). Penerapan Algoritma Rijndael untuk Mengamankan Teks. 02(338), 47–53