PENGAMANAN SQLITE DATABASE MENGGUNAKAN ALGORITMA KRIPTOGRAFI AES DAN RSA BERBASIS ANDROID

Diajukan Sebagai Syarat untuk Menyelesaikan
Pendidikan Program Strata-1 pada
Jurusan Teknik Informatika

Oleh:

Cindy Wijaya

09021281823059

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2022

LEMBAR PENGESAHAN SKRIPSI

PENGAMANAN SQLITE DATABASE MENGGUNAKAN ALGORITMA KRIPTOGRAFI AES DAN RSA BERBASIS ANDROID

Oleh :

Cindy Wijaya
09021281823059

Palembang, 25 Mei 2022

Pembimbing I

Alfarissi, M.Comp.Sc.
NIP. 198512152014041001

Pembimbing II,

Mastura Diana Marieska, M.T.
NIP. 198603212018032001

Mengetahui,
Ketua Jurusan Teknik Informatika,

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI

Pada hari **Jum'at** tanggal **13 Mei 2022** telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Cindy Wijaya
NIM : 09021281823059
Judul : Pengamanan SQLite database menggunakan algoritma kriptografi AES dan RSA berbasis android

dan dinyatakan **LULUS**.

1. Ketua Penguji

   Novi Yusliani, M.T.
   NIP. 198211082012122001 .....

2. Penguji I

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

3. Penguji II

   Hadipurnawan Satria, Ph.D.
   NIP. 198004182020121001 .....

4. Pembimbing I

   Alfarissi, M.Comp.Sc.
   NIP. 198512152014041001 .....

5. Pembimbing II

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

Mengetahui,
Ketua Jurusan Teknik Informatika,

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

HALAMAN PERNYATAAN

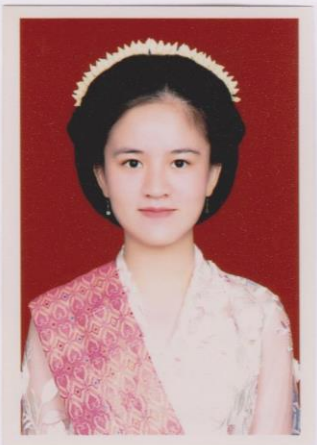
Yang bertanda tangan dibawah ini :

Nama	:	Cindy Wijaya
NIM	:	09021281823059
Program Studi	:	Teknik Informatika Bilingual
Judul Skripsi	:	Pengamanan SQLite Database menggunakan algoritma kriptografi AES dan RSA berbasis android

Hasil pengecekan Software *iThenticate/Turnitin* : 9%

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 Mei 2022

Cindy Wijaya
NIM. 09021281823059

MOTTO DAN PERSEMBAHAN

- Faith and Prayer both are invisible, but they make impossible things possible

Kupersembahkan karya tulis ini kepada :

- Keluargaku
- Teman-teman seperjuangan
- Fakultas Ilmu Komputer
  Universitas Sriwijaya

SQLITE DATABASE SECURITY USING AES AND RSA CRYPTOGRAPHY ALGORITHM ON ANDROID

By:

Cindy Wijaya
09021281823059

ABSTRACT

SQLite database is a lightweight relational database and requires little memory to use, but SQLite database does not have built-in security such as authentication or cryptographic systems. Therefore, this study uses a hybrid cryptosystem with a combination of AES and RSA cryptographic algorithms to secure data stored in the SQLite database. The AES cryptographic algorithm as a symmetric algorithm plays a role in the plaintext encryption and decryption process and the RSA cryptographic algorithm as an asymmetric algorithm plays a role in the process of securing the secret key of the AES algorithm. Based on the results of the study using the number of bits for the RSA algorithm key generation of 2048 bits with an average processing time of 3563 ms, it was found that the combination of the AES and RSA algorithms can increase the security of SQLite databases with an avalanche effect of 50-60%. From the comparative measurement of processing time on SQLite database insert queries, it is found that there is an increase in processing time of 50% when inserting data using a hybrid cryptosystem combination of AES and RSA algorithms.

Keywords: SQLite database, cryptography, hybrid cryptosystem, AES, RSA.

PENGAMANAN SQLITE DATABASE MENGGUNAKAN ALGORITMA KRIPTOGRAFI AES DAN RSA BERBASIS ANDROID

Oleh:

Cindy Wijaya
09021281823059

ABSTRAK

SQLite database merupakan database relational yang ringan dan membutuhkan sedikit memori saat digunakan, namun *SQLite database* tidak memiliki keamanan *built-in* seperti otentikasi atau sistem kriptografi. Oleh karena itu penelitian ini menggunakan *hybrid cryptosystem* dengan kombinasi algoritma kriptografi AES dan RSA untuk mengamankan data yang tersimpan pada *SQLite database.* Algoritma kriptografi AES sebagai algoritma simetri berperan dalam proses enkripsi dan dekripsi *plaintext* dan algoritma kriptografi RSA sebagai algoritma asimetri berperan dalam proses pengamanan *secret key* dari algoritma AES. Berdasarkan hasil penelitian menggunakan jumlah bit pembangkitan kunci algoritma RSA 2048 bit dengan rata-rata *processing time* 3563 ms didapatkan hasil bahwa kombinasi algoritma AES dan RSA dapat meningkatkan keamanan pada *SQLite database* dengan hasil *avalanche effect* sebesar 50-60%. Dari pengukuran perbandingan *processing time* pada *query insert SQLite database* didapatkan hasil bahwa adanya kenaikan *processing time* sebesar 50% pada saat melakukan *insert* data dengan menggunakan *hybrid cryptosystem* kombinasi algoritma AES dan RSA.

Kata kunci: *SQLite database*, kriptografi, *hybrid cryptosystem,* AES, RSA.

KATA PENGANTAR

Puji syukur kepada Tuhan yang Maha Esa atas berkah dan anugerah-Nya sehingga penulis dapat menyelesaikan tugas akhir ini. Tugas akhir yang berjudul "**Pengamanan SQLite database menggunakan algoritma kriptografi AES dan RSA berbasis android**" ini disusun untuk memenuhi salah satu syarat kelulusan tingkat Strata-1 pada Jurusan Teknik Informatika Universitas Sriwijaya.

Penulis menyadari bahwa dalam pengerjaan tugas akhir ini penulis banyak mendapatkan dukungan serta bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan kali ini penulis ingin mengucapkan ucapan terimakasih yang tak terhingga kepada pihak yang telah banyak mendukung dan memberi bantuan, yaitu kepada:

1. Mamaku tersayang Fenia, Papaku Hendy Wijaya, Saudara perempuanku Stefanie Wijaya dan seluruh keluarga besar atas dukungan, bantuan serta doa nya yang diberikan kepada penulis selama ini.
2. Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Ibu Alvi Syahrini Utami, M.Kom. selaku Ketua Jurusan Teknik Informatika yang telah banyak memberikan saran dan informasi selama proses perkuliahan.
4. Bapak Alfarissi, M.Comp.Sc. dan Ibu Mastura Diana Marieska, M.T. selaku pembimbing yang telah membimbing, memberikan motivasi dan banyak membantu penulis dengan sabar.

5. Ibu Desty Rodiah, M.T. selaku pembimbing akademik yang selalu membimbing, memberikan masukan dan motivasi kepada peneliti dalam proses perkuliahan.
6. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Teman seperjuanganku Arya Pradata, Dhiya Calista, Ihtiar Alfath Raden Pangestu, Zora Cahya Ardiya Prameswari dan teman-teman lain yang tidak dapat disebutkan satu-persatu yang telah memberikan semangat dan bantuan kepada penulis.
8. Kak Ichvandi Octa Maulana yang selalu memberikan motivasi dan banyak memberi bantuan kepada penulis dalam menyelesaikan tugas akhir.
9. Teman-teman dari Angkatan TI 2018 khususnya TI Bilingual B, kakak tingkat, adik tingkat, serta teman-teman lain-nya.
10. Dan untuk semua pihak yang telah banyak membantu pengerjaan tugas akhir ini yang tidak dapat disebutkan satu-persatu.

Akhir kata, Penulis sangat menyadari bahwa tugas akhir ini masih jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun dari semua pihak sangat dibutuhkan dalam penyempurnaan tugas akhir ini. Semoga tugas akhir ini bermanfaat bagi semua pihak.

Palembang, 25 Mei 2022

Cindy Wijaya

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I
PENDAHULUAN

1.1 Pendahuluan

Pada Bab I akan dijelaskan mengenai gambaran penelitian ini secara umum. Hal yang akan dibahas yaitu latar belakang masalah, rumusan masalah, tujuan dan manfaat, batasan masalah serta sistematika penulisan.

1.2 Latar Belakang

Penggunaan perangkat mobile telah menjadi bagian dari kehidupan, banyak aplikasi mobile akhirnya menyimpan informasi pengguna di dalam *SQLite database*. *SQLite database* adalah sebuah *open-source relational database* yang digunakan untuk melakukan operasi seperti menyimpan, mengubah, mengambil data pada perangkat android. Menurut (Akowuah, Ahlawat, & Du, 2018) *SQLite database* banyak digunakan karena kebutuhan memori yang kecil, efisiensi penyimpanan tinggi dan menjalankan *query operations* dengan sangat cepat.

(Shekar, 2019) mengemukakan bahwa *SQLite database* dari aplikasi seluler belum cukup aman. Jadi, diperlukan keamanan untuk mengamankan *database* pada aplikasi. (Akowuah, Ahlawat, & Du, 2018) berpendapat bahwa *SQLite database* tersimpan sebagai *cross-platform file* dan data tersimpan secara *plain* (tidak dilindungi dengan enkripsi). Jadi siapa pun yang memiliki akses secara langsung ke file *SQLite*

database dapat membaca atau memodifikasi isi *database*. Sehingga dibutuhkan suatu mekanisme keamanan untuk melindungi data yang tersimpan pada *database*.

Kriptografi merupakan suatu ilmu yang digunakan untuk melindungi keamanan suatu informasi dengan mengonversi data menjadi kode sandi atau menjadi bentuk yang maknanya tidak diketahui. Proses yang ada pada kriptografi terdiri dari dua yaitu enkripsi dan dekripsi. Proses enkripsi adalah proses mengubah informasi asli (*plaintext*) menjadi informasi dalam bentuk sandi (*ciphertext*) sedangkan dekripsi adalah proses mengembalikan informasi dalam bentuk sandi (*ciphertext*) menjadi informasi asli (*plaintext*).

Kriptografi dibagi menjadi dua, yaitu kriptografi kunci simetris dan kriptografi kunci asimetris. Kriptografi kunci simetris menggunakan kunci yang sama untuk melakukan proses enkripsi dan dekripsi contoh nya yaitu AES (*Advanced Encryption Standard*). Sedangkan kriptografi kunci asimetris menggunakan kunci yang berbeda pada proses enkripsi dan dekripsi contohnya yaitu RSA (*Rivest Shamir Adlemen*), algoritma kriptografi RSA ini menggunakan dua buah kunci yaitu kunci publik dan kunci privat, dimana kedua kunci ini dapat diatur panjang nya. Semakin panjang jumlah bit yang digunakan dalam pembangkitan kunci RSA maka semakin aman karena sulit untuk melakukan pemfaktoran pada bilangan yang sangat besar (Khairuzzaman, 2019). Masing-masing algoritma memiliki kelebihan dan kekurangan, algoritma kriptografi kunci simetris memerlukan waktu yang singkat untuk proses enkripsi dan dekripsi

namun kurang pada keamanan kunci nya sedangkan algoritma kriptografi kunci asimetris kebalikannya.

Penelitian ini merupakan penelitian lanjutan dari (Shekar, 2019) yang menggunakan algoritma kunci simetris yaitu AES untuk mengamankan informasi yang tersimpan pada *SQLite database.* Algoritma kriptografi yang digunakan pada penelitian untuk meningkatkan keamanan pada *SQLite database* ini menggunakan gabungan dua algorima yang berbeda yaitu AES dan RSA yang dikenal dengan *Hybrid Cryptosystem*. (Jamaludin, 2018) mengemukakan bahwa *Hybrid Cryptosystem* adalah gabungan antara kriptografi kunci simetris dan kriptografi kunci asimetris. Penggabungan ini dilakukan untuk mengatasi kelemahan masing-masing algoritma.

Pada penggunaan *Hybrid Cryptosystem* ini, algoritma kriptografi RSA sebagai algoritma kriptografi simetri berperan dalam proses enkripsi dan dekripsi *secret key* dari algoritma kriptografi AES sedangkan algoritma kriptografi AES sebagai algoritma kriptografi asimetri berperan dalam proses enkripsi dan dekripsi *plaintext* yang disimpan ke dalam *SQLite Database*. Metode ini diharapkan dapat menghasilkan tingkat keamanan yang tinggi karena untuk dapat membaca informasi harus melalui kombinasi kedua algoritma tersebut.

1.3 Rumusan Masalah

(Akowuah, Ahlawat, & Du, 2018) berpendapat bahwa SQLite *engine*, tidak seperti DBMS *client-server* seperti Oracle dan SQL Server karena SQLite tidak memiliki keamanan *built-in* seperti otentikasi, otorisasi atau sistem kriptografi. Oleh karena itu, bergantung pada lingkungannya untuk menyediakan keamanan yang dibutuhkan. Pernyataan tersebut menjadi pendukung dilakukan nya penelitian ini. Rumusan masalah utama dalam penelitian ini adalah bagaimana cara meningkatkan keamanan data yang tersimpan pada *SQLite database* ?

Agar dapat menjawab rumusan masalah tersebut, pertanyaan pendukung penelitian ini yaitu:

1. Bagaimana implementasi algoritma kriptografi AES dan RSA untuk meningkatkan keamanan data yang tersimpan pada *SQLite database* ?
2. Bagaimana cara menguji keamanan algoritma kriptografi AES dan RSA menggunakan *avalanche effect* ?
3. Bagaimana hasil *processing time* pada proses pembangkitan kunci algoritma RSA jika menggunakan jumlah bit pembangkitan kunci algoritma kriptografi RSA yang berbeda-beda ?
4. Bagaimana hasil perbandingan *processing time* pada *query insert SQLite database* tanpa enkripsi apapun dan dengan menggunakan *hybrid cryptosystem* kombinasi algoritma AES dan RSA ?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Menerapkan *hybrid cryptosystem* dengan melakukan kombinasi algoritma kriptografi AES dan RSA untuk mengamankan data yang tersimpan dalam *SQLite database*.
2. Menguji pengamanan pada kombinasi algoritma kriptografi AES dan RSA menggunakan *avalanche effect*.
3. Melakukan pengukuran *processing time* pada proses pembangkitan kunci algoritma kriptografi RSA dengan menggunakan jumlah bit pembangkitan kunci algoritma kriptografi RSA yang berbeda-beda.
4. Melakukan perbandingan *processing time* pada *query insert SQLite database* tanpa enkripsi apapun dan dengan menggunakan *hybrid cryptosystem* kombinasi algoritma AES dan RSA.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Menghasilkan skema pengamanan *SQLite database* dengan menggunakan *Hybrid Cryptosystem* yang mengombinasikan algoritma kriptografi AES dan RSA.
2. Hasil pada penelitian ini dapat digunakan sebagai acuan untuk penelitian pada keamanan *SQLite database* selanjutnya.

1.6 Batasan Masalah

Batasan masalah dalam penelitian ini adalah:

1. Menggunakan perangkat lunak Android Studio.
2. Inputan data yang ada pada aplikasi berupa teks. Tidak termasuk gambar, file dan lain sebagainya.
3. Menggunakan algoritma kriptografi AES-128.
4. Jumlah bit pembangkit kunci RSA yang digunakan dalam pengujian adalah 256 bit, 512 bit, 1024 bit, 2048 bit dan 4096 bit.
5. Penelitian dikembangkan menggunakan bahasa pemrograman Kotlin.

1.7 Sistematika Penulisan

Sistem penulisan tugas akhir ini sesuai dengan standar penulisan tugas akhir Fakultas Ilmu Komputer Universitas Sriwijaya yaitu :

BAB I. PENDAHULUAN

Bab ini memberikan informasi mengenai latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, serta sistematika penulisan.

BAB II. KAJIAN LITERATUR

Bab II kajian literatur ini menjelaskan dasar-dasar teori yang digunakan dimulai dari penjelasan mengenai kriptografi, *hybrid cryptosystem*, SQLite *database*, AES (*Advanced Encryption Standard*), RSA (*Rivest Shamir*

Adlemen), *Avalanche effect*, android dan menyertakan penelitian yang relevan dengan penelitian ini.

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan Langkah-langkah yang dilakukan dalam penelitian. Setiap tahapan dari rencana penelitian dijelaskan secara rinci sesuai dengan kerangka kerja. Bab ini juga mencakup perancangan manajemen proyek dalam pelaksanaan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Bab ini membahas proses dalam pengembangan perangkat lunak dalam penelitian ini. Metode yang digunakan adalah RUP (*Rational Unified Process*) yang terdiri atas proses *Inception* (Analisis kebutuhan), *Elaboration* (Perancangan sistem), *Construction* (Implementasi perangkat lunak), dan *Transition* (Pengujian perangkat lunak).

BAB V. HASIL DAN ANALISIS PENELITIAN

Pada Bab V akan menjelaskan implementasi hasil analisis dan perancangan yang telah dilakukan sebelumnya. Hasil analisis berupa kesimpulan yag dapat ditarik dari penelitian ini.

BAB VI. KESIMPULAN DAN SARAN

Pada Bab IV terdapat kesimpulan dan saran. Isi pada Bab VI diharapkan dapat membantu meningkatkan dan mengembangkan penelitian selanjutnya.

1.8 Kesimpulan

Kesimpulan yang didapatkan pada Bab 1 ini yaitu masalah yang harus dipecahkan pada penelitian ini adalah bagaimana mengimplementasi algoritma kriptografi AES dan RSA untuk meningkatkan keamanan dan mencegah manipulasi pada data yang tersimpan pada *SQLite Database*, bagaimana cara menguji keamanan kombinasi algoritma AES dan RSA menggunakan *avalanche effect*, bagaimana perbedaan *processing time* pada proses pembangkitan kunci RSA jika menggunakan jumlah bit algoritma RSA yang berbeda-beda, serta bagaimana hasil perbandingan *processing time* pada *query insert SQLite database* tanpa enkripsi apapun dan dengan menggunakan *hybrid cryptosystem*.

DAFTAR PUSTAKA

Adhar, D. (2014). Pengamanan SQLite Database menggunakan Kriptografi Elgamal. *Seminar Nasional Informatika 2014*, 432-436.

Akowuah, F., Ahlawat, A., & Du, W. (2018). Protecting Sensitive Data in Android SQLite Databases Using TrustZone. *Int'l Conf. Security and Management*, 227-228.

Astuti, N. R., Arfiani, I., & Aribowo, E. (2019). Analysis of the security level of modified CBC algorithm cryptography using avalanche effect. *IOP Conference Series: Materials Science and Engineering*, 5.

Hermawan, A., & Ujianto, E. I. (2021). Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA. *InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan*, 326-329.

Irawan, C., & Rachmawanto, E. H. (2021). Keamanan Data Menggunakan Gabungan Kriptografi AES dan RSA. *Proceeding SENDIU 2021*, 567-568.

Jamaludin. (2018). Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem. *Jurnal & Penelitian Teknik Informatika*, 87-88.

Khairuzzaman, M. Q. (2019). Implementasi Kriptografi Kunci Publik dengan Algoritma RSA. *Seminar Nasional Sistem Informasi dan Teknik Informatika*, 219.

Musleha, I., Zain, S., Nawahdah, M., & Salleh, N. (2018). Automatic Generation of Android SQLite Database Components. *ResearchGate*.

Obradovic, N., Kelec, A., & Dujlovic, I. (2019). Performance analysis on Android SQLite database. *18th International Symposium INFOTEH-JAHORINA*.

Shekar, A. R. (2019). Preventing Data Manipulation and Enhancing the Security of data in Fitness Mobile Application. *Second International Conference on Smart Systems and Inventive Technology*, 740-741.

Suhandinata, S., Rizal, R. A., OngkyWijaya, D., Warren, P., & Srinjiwi. (2019). Analisis Performa Kriptografi Hybrid Algoritma Blowfish dan Algoritma RSA. *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)*, 1-5.

Yonathan, F. D., Nasution, H., & Priyanto, H. (2021). Aplikasi Pengaman Dokumen Digital Menggunakan Algoritma Kriptografi Hybrid dan Algoritma Kompresi Huffman. *Jurnal Edukasi dan Penelitian Informatika*, 181-183.

Yusfrizal. (2019). Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper dan RSA Berbasis Android. *Jurnal Teknik Informatika Kaputama (JTIK)*, 31-33.