Available *online* at : http://bit.ly/InfoTekJar

InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan

ISSN (Print) 2540-7597 | ISSN (Online) 2540-7600

Keamanan Komputer

Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA

Aditya Hermawan, Erik Iman Heri Ujianto

Teknologi Informasi Universitas Teknologi Yogyakarta

KEYWORDS

Kriptografi, Enkripsi, Dekripsi, AES, RSA

CORRESPONDENCE

Phone: +62 89673841129

E-mail: aditya.hermawan@student.uty.ac.id

A B S T R A C T

Perkembangan data yang pesat akan membutuhkan keamanan dalam pengiriman data sehingga pihak lain yang tidak diinginkan tidak dapat melihat isi data tersebut. Salah satu cara untuk mengamankan data adalah dengan menggunakan kriptografi. Penelitian ini mengembangkan sebuah aplikasi yang dapat melakukan kombinasi kriptografi yang lebih aman karena pesan yang dikirim harus melalui dua kali proses enkripsi dan dekripsi. Algoritma yang digunakan dalam penelitian ini merupakan gabungan dari algoritma RSA dan algoritma AES. Algoritma RSA digunakan oleh pengirim untuk menghasilkan kunci publik dan pribadi. Algoritma RSA juga digunakan untuk mengenkripsi kunci rahasia, dan algoritma AES digunakan untuk mengenkripsi *plaintext*. Pengirim akan mendapatkan kunci pribadi, kunci rahasia terenkripsi, dan *ciphertext*. Penerima mendekripsi kunci rahasia terlebih dahulu menggunakan algoritma RSA, kemudian mendekripsi *ciphertext* menggunakan algoritma AES dan kunci rahasia.

INTRODUCTION

Teknologi komputer pada saat ini telah mengalami perkembangan yang sangat pesat yang diikuti dengan kumpulan data dan informasi yang besar. Pada penyimpanan data dan informasi, dibutuhkan proses pengamanan agar data dan informasi dapat dilindungi dari berbagai ancaman seperti dapat dengan mudah seseorang melihat, merusak, mencuri ataupun menyalahgunakan data atau informasi penting dari suatu instansi atau perusahaan. Salah satu cara dalam melakukan pengamanan data dan informasi adalah menggunakan teknik kriptografi.

Penelitian [1] membahas mengenai perbandingan kinerja RSA dan AES. Objek yang digunakan yaitu SMS yang dikombinasikan menggunakan algoritma Huffman. Penelitian ini menghasilkan aplikasi kriptografi RSA dan AES berbasis Android dengan fungsi pembangkitan kunci, pengiriman dan penerimaan pesan SMS. Penelitian [2] bertujuan menghasilkan aplikasi yang dapat melakukan enkripsi data menggunakan AES 256 dimana algoritma ini menggunakan prinsip dengan jumlah putaran berdasarkan kunci. Penelitian [3] juga membahas mengenai cara meningkatkan keamanan aplikasi SMS pengaduan kecurangan pemilu sebagai sarana bagi masyarakat untuk melaporkan segala bentuk kecurangan Pemilu yang terjadi kepada KPU dengan aman. Penelitian ini menggunakan metode Algoritma RSA. Aplikasi tersebut mampu menjalankan fungsi pengacakan pesan dengan baik dengan efek *avalanche* sebesar 10.44%. Serangan *brute force* menggunakan *keylength* 16-bit membutuhkan 3,7 milidetik untuk setiap percobaan menemukan 32,768 kemungkinan kunci privat.

Penelitian [4] melakukan analisa dan implementasi kombinasi algoritma Knapsack dan logaritma diskrit pada aplikasi *chat* agar dapat melindungi pesan agar pesan tersebut lebih aman dan tidak mudah dibaca oleh orang yang tidak berhak. Penelitian [5] menghasilkan *prototype* yang dapat melakukan pengamanan ganda terhadap pesan rahasia. Penelitian ini menggunakan teknik steganografi LSB yang dikombinasikan dengan kriptograti Vigenere Cipher. Penelitian [6] menghasilkan aplikasi kriptografi menggunakan algoritma DES dengan input berupa gambar. Hasil penelitian ini menunjukkan panjang kunci untuk algoritma DES harus sepanjang 8 *byte* atau 8 karakter, karena DES adalah algoritma kriptografi *Block Cipher* 64 bit. Sedangkan kunci yang digunakan untuk mendekripsi adalah kunci yang sama dengan kunci saat mengenkripsi. Kelemahan dari algoritma DES sendiri adalah, ketika gambar yang terenkripsi dan dibuka maka akan bertuliskan *Image not supported*, yang akan menimbulkan kecurigaan pada pihak ketiga. Selain itu karena kunci yang digunakan sama, kunci dapat mengalami kebocoran.

Penelitian [7] menggabungkan teknik kriptografi menggunakan metode *Data Encryption Standard* dan teknik steganografi *End of File* dengan cara informasi rahasia dalam bentuk text dienkripsi

https://doi.org/10.30743/infotekjar.v5i2.3585

terlebih dahulu, lalu hasil enkripsi akan dimasukkan ke dalam sebuah citra digital menggunakan format JPEG. Penelitian [8] menggunakan algoritma MD5 untuk teknik tanda tangan digital dan algoritma ElGamal sebagai algoritma kunci publik. Algoritma ElGamal digunakan untuk mengenkripsi intisari pesan dari proses algoritma MD5 ke *file* yang tanda tangan digitalnya merupakan hasil enkripsi intisari pesan. Sedangkan penelitian [9] menerapkan keamanan data *cloud* dengan permasalahan verifikasi data menggunakan algoritma Keccak dan DSA. Jika dibandingkan dengan penelitian sebelumnya dimana algoritma Keccak digunakan pada sistem kerja tanda tangan digital RSA, maka sistem kerja tanda tangan DSA yang menggunakan algoritma Keccak lebih baik dalam hal waktu pelaksanaan proses penandatanganan, tetapi untuk verifikasi perbandingan, proses eksekusi RSA lebih cepat dari pada DSA. Penelitian [10] membuat sistem yang dapat mengamankan *e-mail* sebelum dilakukannya proses pengiriman, dengan cara melakukan enkripsi pada email tersebut menggunakan metode kriptografi Blowfish, kemudian mengenkripsi kunci simetris menggunakan kriptografi RSA.

Ide utama dari penelitian ini adalah melakukan perancangan dan implementasi enkripsi data menggunakan algoritma RSA dan algoritma AES. Maka berdasarkan uraian di atas, dilakukan implementasi kombinasi antara algoritma RSA dan algoritma AES yang diharapkan dapat menghasilkan pesan rahasia yang lebih aman karena dalam proses membaca isi pesan rahasia harus melalui kedua algoritma kombinasi tersebut. Mekanisme yang dilakukan yaitu menggunakan algoritma AES untuk melakukan enkripsi pada data. Kemudian untuk mendapatkan kunci rahasia yang diperlukan untuk mendekripsi data tersebut, penerima menerbitkan kunci publik dengan mempertahankan kunci pribadi yang hanya penerima dan pengirim ketahui. Pengirim kemudian menggunakan kunci pribadi dan alogritme RSA untuk mengenkripsi dan mengirimkan setiap penerima kunci pribadi AES sendiri yang dapat digunakan untuk mendekripsi data tersebut.

METHOD

A. Studi Literatur

Membaca dan mengkaji beberapa literatur tentang teori-teori dasar yang mendukung penelitian ini dengan mencari buku-buku di jaringan komputer, jurnal, artikel internet, tutorial dan catatan video yang ada hubungannya dengan enkripsi dan dekripsi menggunakan algoritma RSA dan AES.

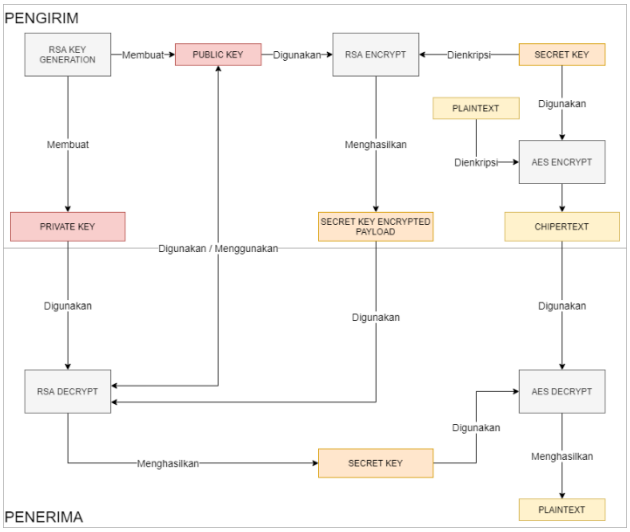
B. Desain Percobaan

Penelitian ini mencoba mengimplementasikan perancangan aplikasi yang dapat melakukan kombinasi algoritma dengan cara membuat kunci publik dan kunci pribadi serta enkripsi dan dekripsi menggunakan RSA dan AES.
Untuk menunjang kelancaran penelitian yang dilakukan, hal pertama yang dilakukan adalah mencari dan mengumpulkan berbagai literatur yang mengarah pada berbagai metode kriptografi dan aspek pendukung lainnya. Selanjutnya perancangan aplikasi yang akan mengimplementasikan kombinasi antara algoritma RSA dan AES. Dalam melaksanakan penelitian ini secara lebih rinci, metode yang akan dilakukan ditunjukkan pada Gambar 1 Rangkaian Tahapan Penelitian.

Gambar 1. Rangkaian Tahapan Penelitian

C. Pemodelan Sistem

Sebelum melakukan perancangan aplikasi, diperlukan pemodelan sistem agar penelitian ini dapat mencapai tujuannya yaitu dapat menghasilkan pesan rahasia yang lebih aman. Pemodelan sistem ditunjukkan pada Gambar 2 Pemodelan Sistem.



Gambar 2. Pemodelan Sistem

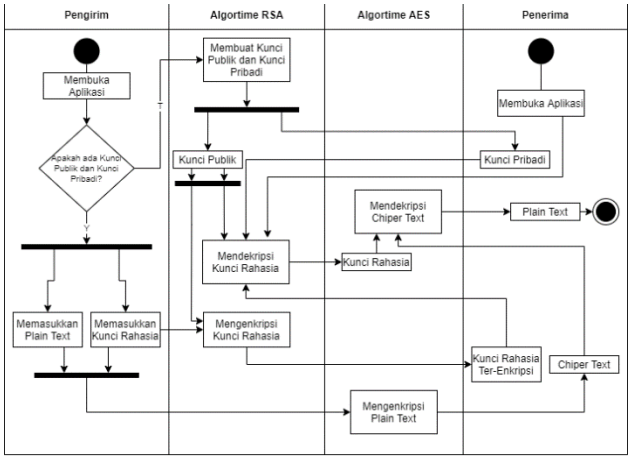
Pada pemodelan sistem, pengirim menerbitkan kunci publik dan kunci pribadi. Kemudian kunci publik tersebut digunakan pada algoritma RSA beserta kunci rahasia yang pengirim buat untuk dienkripsi. Hasil keluaran dari enkripsi RSA tersebut yaitu kunci rahasia yang sudah terenkripsi. Selanjutnya pengirim mengenkripsi *plaintext* atau pesan rahasia menggunakan algoritma AES yang akan dikirim ke penerima menggunakan kunci rahasia sebelum terenkripsi sehingga menghasilkan

https://doi.org/10.30743/infotekjar.v5i2.3585

ciphertext. Penerima mengirimkan kunci pribadi, kunci rahasia terenkripsi dan *ciphertext* kepada penerima.
Penerima akan mendekripsi terlebih dahulu kunci rahasia menggunakan metode RSA dengan bantuan kunci pribadi sehingga menghasilkan kunci rahasia yang sudah terdekripsi. Selanjutnya penerima melakukan dekripsi terhadap *ciphertext* menggunakan metode AES dengan bantuan kunci rahasia yang sudah terdekripsi tersebut, sehingga isi pesan rahasia yang diterima penerima dapat terbaca.
Kombinasi pemodelan sistem yang menggabungkan algoritma AES dan algoritma RSA akan mempersulit pihak lain selain penerima sebenarnya yang akan membaca pesan rahasia tersebut. Hal tersebut dikarenakan untuk membaca pesan rahasia tersebut dibutuhkan dua kali dekripsi, yaitu dekripsi kunci rahasia menggunakan metode RSA dan dekripsi *ciphertext* menggunakan metode AES.

D. Perancangan Aplikasi

Perancangan aplikasi digunakan untuk memudahkan penelitian ini dalam menerapkan pemodelan sistem yang telah dibuat sebelumnya pada aplikasi yang akan dibuat. Perancangan aplikasi hanya menggunakan *activity diagram* yang ditunjukkan pada Gambar 3 *Activity Diagram*.



Gambar 3. *Activity Diagram*

Perancangan aplikasi hanya menggunakan activity diagram dikarenakan dalam perancangan aplikasi ini tidak membutuhkan *database*. Penelitian ini berfokus terhadap implementasi metode kombinasi yang digunakan yaitu algoritma AES dan algoritma RSA. Masukan yang dibutuhkan pengirim yaitu *plaintext* dan kunci rahasia. Sistem akan secara otomatis membuat kunci publik dan kunci pribadi yang akan digunakan untuk mengenkripsi dan mendekripsi kunci rahasia. Keluaran yang diterima pengirim adalah kunci rahasia terenkripsi, kunci pribadi dan *ciphertext*. Semua keluaran tersebut akan diberikan kepada penerima.
Sedangkan penerima memasukkan kunci rahasia terenkripsi, kunci pribadi dan *ciphertext* ke dalam sistem. Sistem akan mendekripsi kunci rahasia dan *ciphertext* yang dimasukkan tersebut. Keluaran yang diterima pengirim adalah *plaintext* atau pesan rahasia yang dikirim oleh pengirim.

E. Data Uji Coba

Data yang digunakan dalam penelitian ini berupa *plaintext* dan kunci rahasia yang akan dimasukkan ke sistem yang ditunjukkan pada Tabel 1 Data Uji Coba.

Tabel 1. Data Uji Coba

Uji Coba ke-	***Plaintext***	**Kunci Rahasia**
1	Bukan Pesan Rahasia	pesan rahasia
2	ini pesan rahasia	Add19GKkF!S AS333F
3	adityahermawan.my.id	S3g0Goyeng!
4	Okeaditya988	H3r11!4w@n
5	Universitas Teknologi Yogyakarta	YUjX4H79qfke LPD8GNqFYC 4gU9f3LPz4

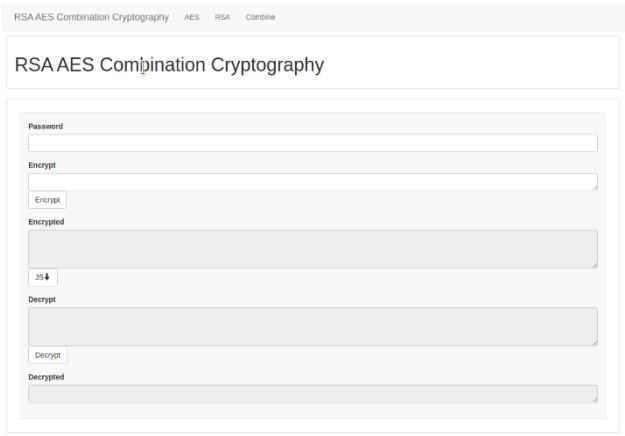
RESULTS AND DISCUSSION

A. Hasil Implementasi Aplikasi

Pada hasil implementasi aplikasi dilakukan penerjemahan dari perancangan aplikasi dengan menggunakan bahasa pemrograman PHP dan Javascript menjadi beberapa fungsi, sehingga dapat dimengerti oleh perangkat komputer untuk mengeksekusi suatu proses.

Halaman AES

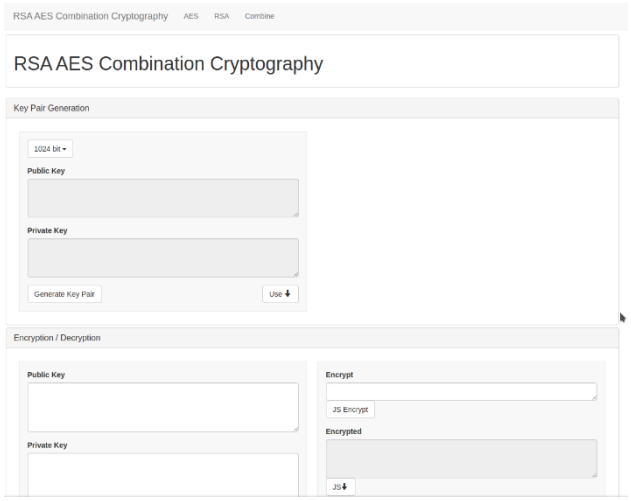
Aplikasi kombinasi algoritma AES dan RSA dijalankan melalui *web browser*. Pada halaman utama akan tampil beberapa menu yaitu AES, RSA, dan *Combine*. Sedangkan halaman yang muncul pertama kali yaitu halaman pada menu AES yang ditunjukkan pada Gambar 4 Halaman AES. Halaman ini hanya berfungsi sebagai enkripsi dan dekripsi menggunakan algoritma AES.



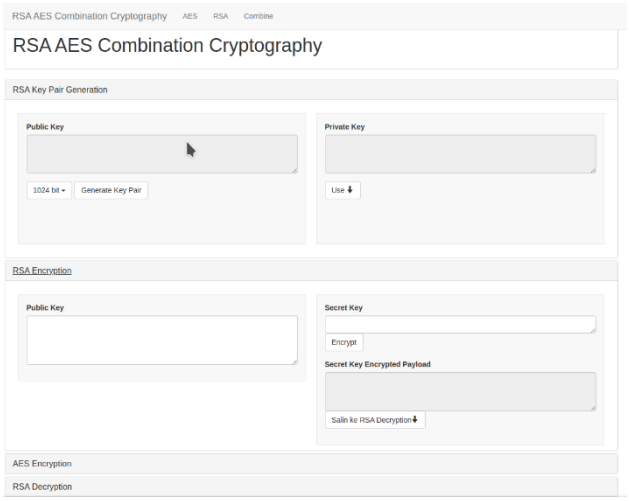
Gambar 4. Halaman AES

Halaman RSA

Halaman RSA merupakan halaman yang digunakan untuk pembangkitan kunci privat dan kunci publik enkripsi dan dekripsi menggunakan algoritma RSA yang ditunjukkan pada Gambar 5 Halaman RSA.



Gambar 5. Halaman RSA



Gambar 6. Halaman *Combine*

Halaman Combine

Halaman *Combine* merupakan halaman yang digunakan pada penelitian ini. Halaman Combine memiliki fungsi yang sama dari dua menu sebelumnya yaitu RSA dan AES. Halaman ini disesuaikan dengan perancangan aplikasi yang telah dibuat sebelumnya. Terdapat beberapa bagian yang digunakan pada halaman ini yaitu RSA *Key Pair Generation*, RSA *Encryption*, AES *Encryption*, RSA *Decryption*, dan bagian terakhir yaitu AES *Decryption* yang ditunjukkan pada Gambar 6 Halaman *Combine*.

B. Hasil Pengujian Sistem

Pengujian sistem yang dilakukan yaitu pengujian *black box*, pengujian pembangkitan kunci dan pengujian data.

Pengujian Black Box

Proses yang dijadikan objek pada pengujian black box ini terdiri dari proses RSA *Key Pair Generation*, RSA *Encryption*, AES *Encryption*, RSA *Decryption*, dan AES *Decryption* yang ditunjukkan pada Tabel 2 Hasil Pengujian *Black Box.*

Tabel 2. Hasil Pengujian Black Box

Skenario	**Hasil Diharapkan**	**Hasil**
Pengirim memilih *bit generation key*, kemudian menekan tombol *Generate Key Pair*	Menghasilkan *public key* dan *private key*	Diterima
Pengirim memasukkan *secret key*, kemudian menekan tombol *Encrypt*	Menghasilkan *secret key encrypted payload*	Diterima
Pengirim memasukkan *plaintext* dan *secret key* yang digunakan sebelumnya, kemudian menekan tombol *Encrypt*	Menghasilkan *ciphertext*	Diterima
Penerima memasukkan *private key* dan *secret key encrypted payload*, kemudian menekan tombol *Decrypt*	Menghasilkan *ciphertext*	Diterima
Penerima memasukkan sembarang *private key* dan *secret key encrypted payload*, kemudian menekan tombol *Decrypt*	Menamplikan kesalahan pada *console*	Diterima
Penerima memasukkan *secret key* dan *ciphertext*, kemudian menekan tombol *Decrypt*	Mengasilkan *plaintext*	Diterima
Penerima memasukkan sembarang *secret key* dan sembarang *ciphertext*, kemudian menekan tombol *Decrypt*	Menamplikan kesalahan pada *console*	Diterima

Berdasarkan hasil pengujian *black box* dapat disimpulkan bahwa sistem yang dikembangkan dapat mengetahui proses yang benar dan salah, sehingga secara fungsional mengeluarkan hasil yang sesuai dengan diharapkan dalam penelitian ini.

Pengujian Pembangkitan Kunci

Sebelum dilakukan pengujian data, dilakukan dahulu pengujian terhadap pembangkitan kunci privat dan kunci publik. Pembangkitan kunci menggunakan empat jenis bit yaitu 512, 1024, 2048, dan 4096 bit. Hasil pengujian pembangkitan kunci ditunjukkan pada Tabel 3 Hasil Pengujian Pembangkitan Kunci.

Tabel 3. Hasil Pengujian Pembangkitan Kunci

Bit	**Waktu Proses (ms)**	**Hasil**
512	113,29	Dapat menghasilkan kunci publik sepanjang 128 karakter dan kunci privat sepanjang 424 karakter
1024	203,345	Dapat menghasilkan kunci publik sepanjang 216 karakter dan kunci privat sepanjang 812 karakter
2048	495,56	Dapat menghasilkan kunci publik sepanjang 392 karakter dan kunci privat sepanjang 1592 karakter
4096	13521,615	Dapat menghasilkan kunci publik sepanjang 736 karakter dan kunci privat sepanjang 3132 karakter

https://doi.org/10.30743/infotekjar.v5i2.3585

Berdasarkan hasil pengujian pembangkitan kunci dapat ditunjukkan bahwa terdapat perbedaan yang signifikan antara 2048 bit dengan 4096 bit yaitu 495,56 ms dan 13521,615 ms sehingga peneliti menggunakan 2048 bit sebagai jenis bit yang akan digunakan dalam proses enkripsi dan dekripsi RSA.

Pengujian Data

Setelah dilakukan pengujian pembangkitan kunci, peneliti dapat melakukan pengujian terhadap data yang akan digunakan. Hasil pengujian data ditunjukkan pada Tabel 4 Hasil Pengujian Enkripsi Data dan Tabel 5 Hasil Pengujian Dekripsi Data.

Tabel 4. Hasil Pengujian Enkripsi Data

Data ke-	**Waktu Enkripsi RSA (ms)**	**Waktu Enkripsi AES (ms)**	**Hasil**
1	5,385	11,675	Masukan yang diharapkan dapat diterima yaitu 'Bukan Pesan Rahasia'
2	5,305	3,46	Masukan yang diharapkan dapat diterima yaitu 'ini pesan rahasia'
3	5,895	3,11	Masukan yang diharapkan dapat diterima yaitu 'adityahermawan.my.id'
4	5,41	1,65	Masukan yang diharapkan dapat diterima yaitu 'Okeaditya988'
5	15,145	1,93	Masukan yang diharapkan dapat diterima yaitu 'Universitas Teknologi Yogyakarta'
Rata - Rata	**7,428**	**4,365**	

Berdasarkan hasil pengujian enkripsi data dapat disimpulkan bahwa sistem dapat melakukan proses enkripsi *secret key* menggunakan algoritma RSA dan proses enkripsi *plaintext* menggunakan algoritma AES. Sedangkan pada hasil pengujian enkripsi data di atas, rata-rata waktu yang digunakan pada proses enkripsi sangat cepat yaitu 7,428 ms pada proses enkripsi RSA dan 4,365 ms pada proses enkripsi AES.

Tabel 5. Hasil Pengujian Dekripsi Data

Data ke-	Waktu Dekripsi RSA (ms)	Waktu Dekripsi AES (ms)	Hasil
1	57,345	3,285	Keluaran yang diharapkan dapat diterima yaitu 'Bukan Pesan Rahasia'
2	66,155	4,06	Keluaran yang diharapkan dapat diterima yaitu 'ini pesan rahasia'
3	60,725	1,7	Keluaran yang diharapkan dapat diterima yaitu 'adityahermawan.my.id'
4	25,355	3,305	Keluaran yang diharapkan dapat diterima yaitu 'Okeaditya988'
5	60,76	1,415	Keluaran yang diharapkan dapat diterima yaitu 'Universitas Teknologi Yogyakarta'
Rata - Rata	**54,068**	**2,753**	

Berdasarkan hasil pengujian dekripsi data dapat disimpulkan bahwa sistem dapat melakukan proses dekripsi *secret key encrypted payload* menggunakan algoritma RSA dan proses dekripsi *ciphertext* menggunakan algoritma AES. Sedangkan pada hasil pengujian dekripsi data di atas, rata-rata waktu yang digunakan pada proses dekripsi lebih lambat dibandingkan dengan proses enkripsi yaitu 54,068 ms pada proses dekripsi RSA, sedangkan pada proses dekripsi AES lebih cepat dibandingkan proses enkripsi 2,753 ms.

CONCLUSIONS

A. Kesimpulan

Penelitian implementasi enkripsi data menggunakan kombinasi AES dan RSA yang memiliki tipe enkripsi yang berbeda, yaitu simetris dan asimetris dapat diterapkan untuk mengenkripsi dan mendekripsi data dengan aman. Hal ini dikarenakan diperlukan dua kali proses dekripsi dan menggunakan kunci pribadi untuk mendapatkan informasi pesan rahasia tersebut. Pembangkitan kunci yang ideal digunakan yaitu 2048 bit dengan waktu pembuatan yaitu 495,56 ms. Proses dekripsi membutuhkan waktu lebih lama dibandingkan proses enkripsi. Proses enkripsi menggunakan RSA membutuhkan waktu rata-rata 7,428 ms dan proses enkripsi menggunakan AES membutuhkan waktu rata-rata 4,365 ms. Sedangkan proses dekripsi menggunakan RSA membutuhkan waktu rata-rata 54,068 ms dan proses dekripsi menggunakan AES membutuhkan waktu rata-rata 2,753 ms.

B. Saran

Penelitian ini masih memiliki kekurangan dan memerlukan penelitian lanjutan guna menyempurnakannya. Beberapa hal yang perlu penelitian lanjutan yaitu sebagai berikut:

1. Penelitian ini dapat dilanjutkan dengan meningkatkan keamanan dengan menerapkan metode kombinasi yang lebih kompleks dari AES dan RSA.
2. Penelitian dapat dilanjutkan dengan menambahkan kemampuan aplikasi untuk dapat menyisipkan pesan rahasia pada media lain seperti suara, video dan *file* berformat lainnya.

REFERENCES

[1] L. Laurentinus, H. A. Pradana, D. Y. Sylfania, and F. P. Juniawan, "Perbandingan kinerja RSA dan AES terhadap kompresi pesan SMS menggunakan algoritma Huffman", *Jurnal Teknologi dan Sistem Komputer*, vol. 8, no. 3, pp. 171-177, 2020.

[2] Y. Wiharto and A. Irawan, "Enkripsi Data Menggunakan Advanced Encryption Standard 256", *Jurnal Kilat*, vol. 7, no. 2, pp. 91-99, 2018.
[3] D. Y. Sylfania, F. P. Juniawan, L. Laurentinus, and H. A. Pradana, "SMS Security Improvement using RSA in Complaints Application on Regional Head Election's Fraud", *Jurnal Teknologi dan Sistem Komputer*, vol. 7, no. 3, pp. 116-120, 2019.
[4] Aminudin, A. H. Helmi, and S. Arifianto, "Analisa Kombinasi Algoritma Merkle-Hellman Knapsack dan Logaritma Diskrit pada Aplikasi Chat", *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 5, no. 3, pp. 325-333, 2018.
[5] A. Wibowo, "Prototype 'Pengamanan Ganda' Pesan Rahasia dengan Menggunakan Teknik Steganografi Metode LSB dan Kriptografi Metode Vigenere Cipher", *Jurnal Teknik Informatika*, vol. 1, no. 2, pp. 1-16, 2017.
[6] A. A. Permana, and D. Nurnaningsih, "Prototype Application of Cryptography with Data Encryption Standard (DES) Algorithm in Picture", *Jurnal Informatika*, vol. 4, no. 2, pp. 9-14, 2020.
[7] D. Darwis, Wamiliana, A. Junaidi, "Proses Pengamanan Data Menggunakan Kombinasi Metode Kriptografi Data Encryption Standard dan Steganografi End of File", *Prosiding Seminar Nasional Metode Kuantitatif*, 24-25 November 2017, Lampung: UNILA, 2017.
[8] M. Iqbal, A. P. U. Siahaan, and R. P. Sundari, "Combination of MD5 and ElGamal in Verifying File Authenticity and Improving Data Security", *International Journal for Innovative Research in Multidisciplinary Field*, vol. 4, no. 10, pp. 96-101, 2018.
[9] M. A. Nazal, R. Pulungan, and M. Riasetiawan, "Data Integrity and Security using Keccak and Digital Signature Algorithm (DSA)", *Indonesian Journal of Computing and Cybernetics Systems*, vol. 13, no. 3, pp 273-282, 2019.
[10] M. I., Zulfikar, G., Abdillah, and A., Komarudin, "Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA)", *Seminar Nasional Aplikasi Teknologi Informasi (SNATi)*, 03 Agustus 2019, Yogyakarta: UII, 2019.

 https://doi.org/10.30743/infotekjar.v5i2.3585