ALGORITMA: Jurnal Ilmu Komputer dan Informatika
Volume: 06, Number: 01, April 2022 ISSN 2598-6341 (online)

Implementasi Kriptografi Hybrida Algoritma RSA dan Vernam Cipher Dalam Pengamanan File Text

Hori Andara[1], Fera Damayanti[2], Khairunnisa[3]
[1,2,3]Program Studi Teknik Informatika Fakultas Teknik dan Komputer
Universitas Harapan Medan
Jl. H.M. Jhoni No 70 Medan, Indonesia
Hori.andara02@gmail.com[1], Feradamayantii@gmail.com[2], Khairunnisajv2@gmail.com[3]

Abstract

Nowadays, The development of the times is in line with the development of computer technology, which means that the storage and delivery of electronic documents is also increasing rapidly. Text files as a form of representation of electronic documents, namely all electronic information created and stored in digital form. The issue of information security in text files is a very crucial issue to be discussed. Especially if the text file sent has important and confidential information. If ignored, the information can be changed or used by irresponsible parties. Therefore, we need a technique or method to maintain the confidentiality of information known as cryptography. Cryptography has two key types, namely symmetric and asymmetric. In this study, the authors combine symmetric and asymmetric keys. The symmetric key has one key, while the asymmetric key has two keys,namely the public key and the private key. Symmetric keys are used to secure text files, while asymmetric keys are used to secure symmetric keys, a process known as hybrid cryptosystem. One of the symmetric algorithms is Vernam Cipher, while the RSA algorithm is one of the asymmetric algorithms. Secured text files are those with the *.txt file format. The results of the system testing in this study show that the time required for text file encryption is directly proportional to the character length of the text file. This means that the longer the text file used, the longer it will take to encrypt and decrypt the text file.

Keywords: Cryptopraphy, Hybrid Cryptosystem, Vernam Cipher, RSA

Abstrak

Perkembangan zaman selaras dengan perkembangan teknologi komputer, yang berarti penyimpanan dan pengiriman dengan dokumen elektronik juga meningkat pesat. File teks sebagai bentuk representasi dari dokumen eleketronik yaitu segala informasi elektronik yang dibuat dan disimpan dalam bentuk digital. Masalah keamanan informasi didalam file teks menjadi isu yang sangat krusial untuk dibahas. Terutama apabila file teks yang dikirimmemiliki informasi penting dan rahasia. Apabila diabaikan, informasi tersebut dapat dirubah atau dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Oleh karena itu, diperlukan suatu teknik atau metode untuk menjaga kerahasiaan informasi yang dikenal dengan istilah kriptografi. Kriptografi memiliki dua tipe kunci yaitu simetris dan asimetris. Pada penelitian ini penulis menggabungkan kunci simetris dan asimetris. Kunci simetris memiliki satu kunci, sedangkan asimetris memiliki dua kunci yaitu kunci publik dan kunci private. Kunci simetris digunakan untuk mengamankan file teks, sedangkan kunci asimetris digunakkan untuk mengamankan kunci simetris, proses ini yang disebut dengan hybrid cryptosystem. Salah satu algoritma simetris adalah Vernam Cipher, sedangkan algoritma RSA adalah salah satu algoritma asimetris. File teks yang diamankan adalah yang memiliki format file *.txt. Hasil dari pengujian sistem pada penelitian ini menunjukakan proses waktu yang dibutuhkan untuk enkripsi file teks dengan berbanding lurus dengan panjang

karakter file teks. Artinya semakin panjang file teks yang digunakan maka akan semakin lama juga waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi pada file teks tersebut.

Kata Kunci : Kriptografi, Kriptografi Hybrid, Vernam Cipher, RSA

1. PENDAHULUAN

Perkembangan zaman selaras dengan perkembangan teknologi komputer, yang berarti penyimpanan dan pengiriman dengan dokumen elektronik juga meningkat pesat. *File* teks sebagai bentuk representasi dari dokumen eleketronik yaitu segala informasi elektronik yang dibuat dan disimpan dalam bentuk digital. *File* teks merupakan berkas yang mengandung informasi-informasi dalam bentuk teks yang terdiri dari karakter, angka dan tanda baca. Informasi yang terdapat didalam dokumen dapat berupa informasi penting bahkan rahasia. Karena itu *file* teks suatu hal yang bisa ditemukan dimana-mana yang disimpan menggunakan komputer atau perangkat elektronik lainnya untuk menampilkan maupun memprosesnya. *File* teks memiliki berbagai format, salah satunya yaitu format data teks (**.txt*).

Kriptografi adalah suatu cabang ilmu yang memelajari cara atau metode matematika yang berkaitan dengan aspek keamanan informasi misal otentikasi, integritas data, serta kerahasiaan. Berdasarkan kuncinya algoritma kriptografi memiliki dua tipe yaitualgoritma kriptografi asimetris dan simetris. Dalam proses enkripsi dan dekripsi kriptografikunci simetris, kunci yang sama digunakan sehingga kerahasiaan kunci dapat dijamin dan tersembunyi. Kriptografi kunci asimetris memiliki kunci yang berbeda dalam proses enkripsi dan dekripsi, dikenal dengan nekripsi kunci public.[1]

Algoritma kriptografi *Vernam Cipher* merupakan algoritma kriptografi berjenis *symmetic key*. Kunci yang digunakan untuk melakukan enkripsi dan deksripsi menggunakan kunci yang sama.dalam melakukan enkripsi, algoritma *Vernam Cipher* menggunakan cara *stream cipher* dimana *cipher* berasal dari hasil operasi *XOR* antara *bit plaintex*t dan *bit key*.[2] Sedangkan algoritma RSA (Rivest Shamir Adleman) merupakan blok *cipher* dimana semua informasi dipetakan ke sebuah *intege*r. Algoritma RSA terdiri dari kunci publik dan kunci *private* dimana kunci publik dapat diketahui oleh semua orang sedangkan kunci *private* hanya diketahui oleh pemilik data. Proses enkripsi menggunakan kunci publik dan proses dekripsi menggunakan kunci *private* pemilik data.[1]

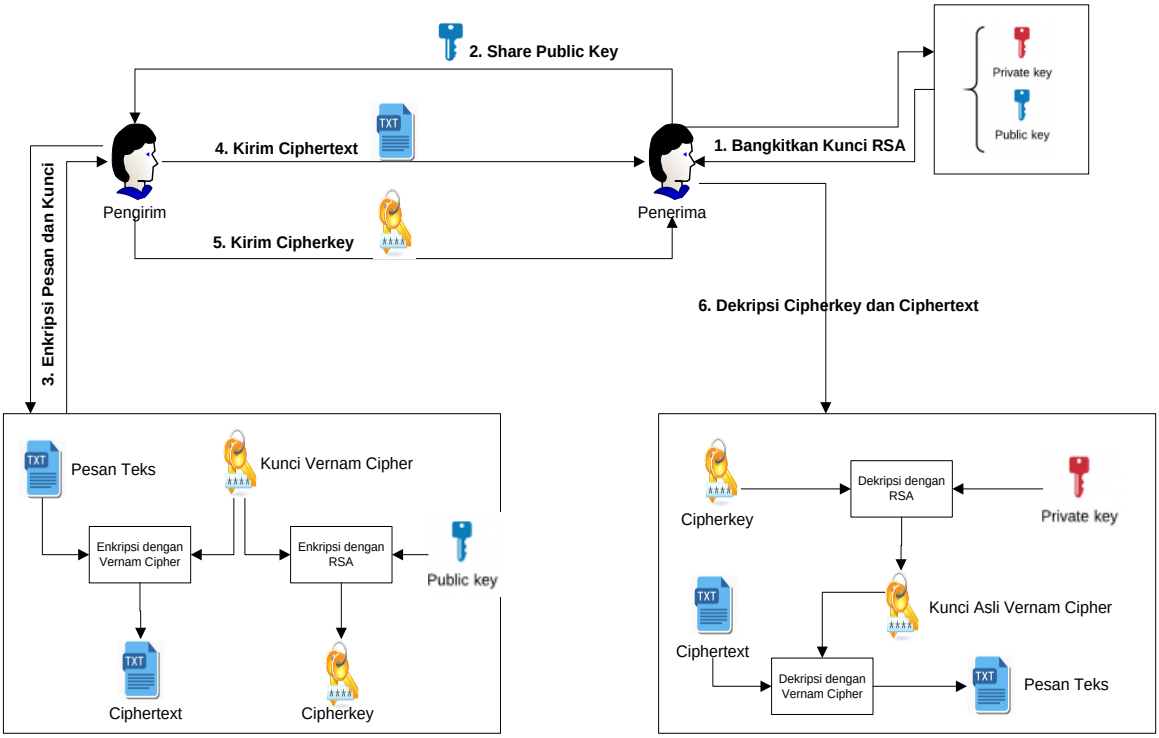
Penelitian terkait yang relevan dengan pokok permasaahan dalam peneitian ini seperti yang dilakukan oleh [3] dengan mengkombinasikan algoritma *Vernam Cipher* dan algoritma *Playfair Cipher*. Kedua algoritma ini dikombinasikan agar *ciphertext* yang dihasilkan lebih sulit untuk dipecahkan oleh kriptanalis karena *cipher* teks yang dihasilkan dari algoritma pertama akan diproses kembali menjadi cipherteks kedua sehingga akan lebih memperumit kode yang dihasilkan.

Berdasarkan hal tersebut, maka penulis bermaksud untuk mengombinasikan algoritma RSA dengan algoritma simetris *Vernam Cipher* sehingga menghasilkan *ciphertext* yang panjangnya sama dengan *plaintext* secara *hybrid cryptosystem* untuk mengamankan data. *Hybrid cryptosystem* merupakan suatu cara atau metode untuk mengkombinasikan algoritma simetris dan algoritma asimetris dengan menggunakan kelebihan dari masing-masing algoritma. *Hybrid cryposystem* dapat memberikan

keamananyang baik dengan operasi waktu yang lebih cepat. Berdasar penjelasan dan paparan sebelumnya, sehingga penulis ingin melakukan penelitian tugas akhir dengan judul "Implementasi Kriptografi *Hybrida* Algoritma RSA dan *Vernam Cipher* Dalam Pengamanan *File* Teks".

2. METODOLOGI PENELITIAN

Dalam perangkat lunak yang akan dibangun, pesan teks diamankan melalui enkripsi dengan mengkombinasikan algoritma simetris *Vernam Cipher* dengan algoritma asimetris RSA secara *hybrid cryptosystem* seperti digambarkan pada skema berikut:



Gambar 1 Skema Enkripsi dan Dekripsi Metode Hybrid Vernam Cipher dan RSA

Pada gambar 1 diatas, pertama penerima akan membangkitkan kunci publik dan kunci privat algoritma RSA, selanjutnya penerima akan mengirimkan kunci publik ke pengirim. Setelah itu pengirim akan mengenkripsi pesan dengan menggunakan kunci algoritma *Vernam Cipher* serta mengenkripsi kunci dengan menggunakan kunci publik.

Algoritma RSA sehingga akan menghasilkan *ciphertext* dan *cipherkey*, yang selanjutnya akan dikirimkan ke penerima. Penerima akan mengenkripsi *cpherkey* terlebih dahulu dengan mnggunakan kunci privat algortitma RSA untuk mendapatkan kunci asli *Vernam Cipher*. Setelah itu barulah penerima dapat mengenkripsi *ciphertext* dengan menggunakan kunci asli *Vernam Cipher* sehingga akan menghasilkan pesan teks asli yang dapat dipahamioleh penerima pesan.

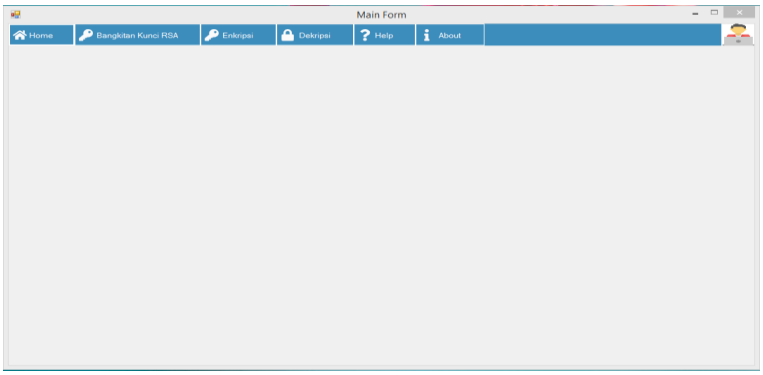
3. Hasil dan Pembahasan

Sesudah sistem dianalisis serta didesain secara rinci, sehingga akan mengarah sesi implementasi. Pada implementasi ini menggunakan teknik *Hybrid Cryptosystem* dengan menggunakan dua algoritma yang termasuk kedalam algoritma simetris dan asimetris yaitualgoritma *Vernam Cipher* dan algoritma RSA yang digunkan untuk pengamanan *file* teks yang dikhususkan *file* dengan *format **.txt*. Sistem ini akan dibangun menggunakan bahasa pemrograman *C#* dalam perangkat lunak *Microsoft Visual Studio*. Spesifikasi perangkat keras yang digunakan dalam pembangunan sistem dan pengujian sistem yang akan dilakukan adalah sebagai berikut:

1) CPU : *Intel(R) Pentium(R) Core(TM) i3-380M @ 2.13 GHz*
2) RAM : 2 GB
3) Monitor : 14 Inc
4) Sistem Operasi : *Windows 7 Ultimate*

3.1 Tampilan Form Utama

Tampilan ini merupakan tampilan awal saat sistem pertama kali dijalankan. Pada *form* ini terdapat pilihan menu untuk bangkit kunci, menu enkripsi, menu dekripsi, menu *help*, dan menu about.



Gambar 2 Form Utama

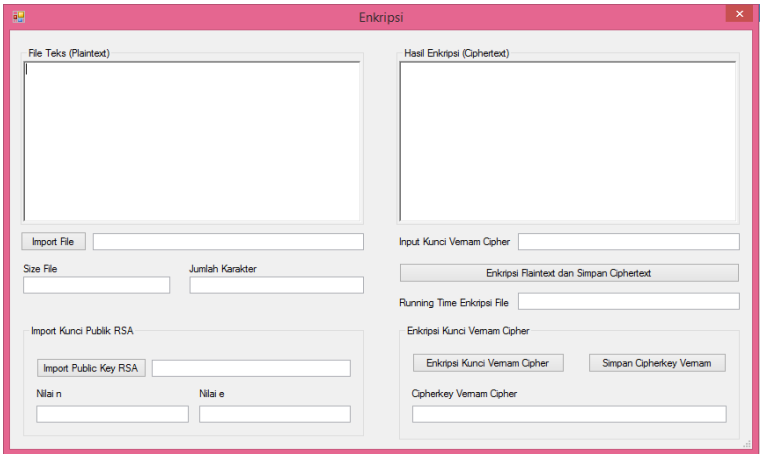
3.2 Tampilan Form Bangkit Kunci

Pada tampilan *form* bangkit kunci merupakan implementasi dari algoritma RSA untuk membangkitkan kunci publik dan kunci privat.

Gambar 3 Form Bangkit Kunci

3.3 Tampilan Form Enskripsi

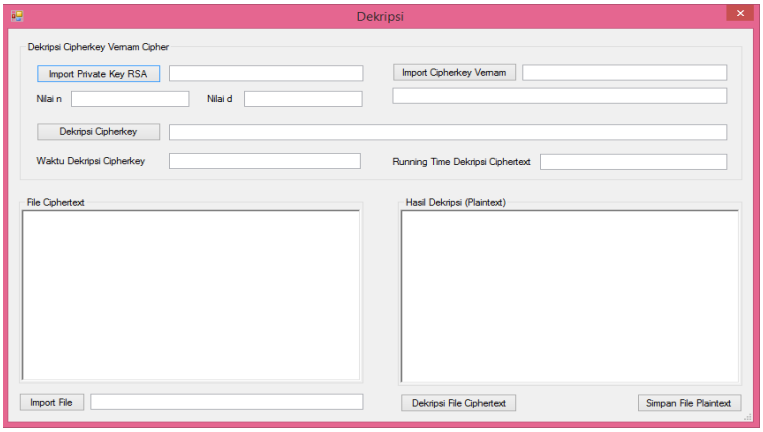
Pada *form* enkripsi merupakan proses untuk penyandian pesan dan kunci. Pada *form* ini memiliki dua proses, yang pertama untuk enkripsi pesan (*plaintext*) menggunakan algoritma *Vernam Cipher*, yang kedua mengenkripsi kunci *Vernam Cipher* menggunakan kunci publik algoritma RSA.



Gambar 4 Form Enskripsi

3.4 Tampilan Form Deskripsi

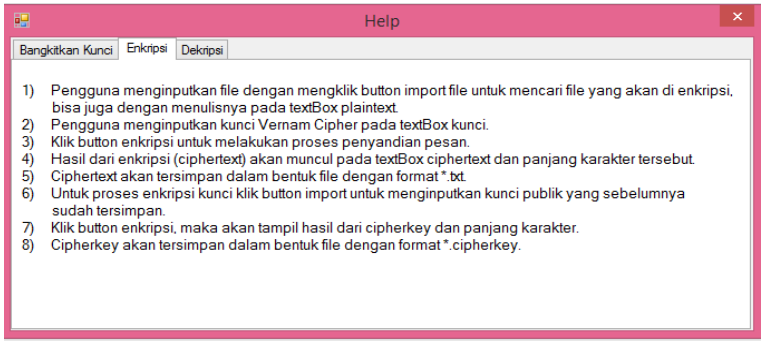
Pada tampilan *form* ini merupakan proses untuk mengembalikan pesan dan kunci yang sudah tersandi kembali ke bentuk awal. Pada proses dekripsi kunci akan menggunakan algoritma yang sama dengan dekripsi yaitu algoritma RSA.



Gambar 5 Form Deskripsi

3.5 Tampilan Form Help

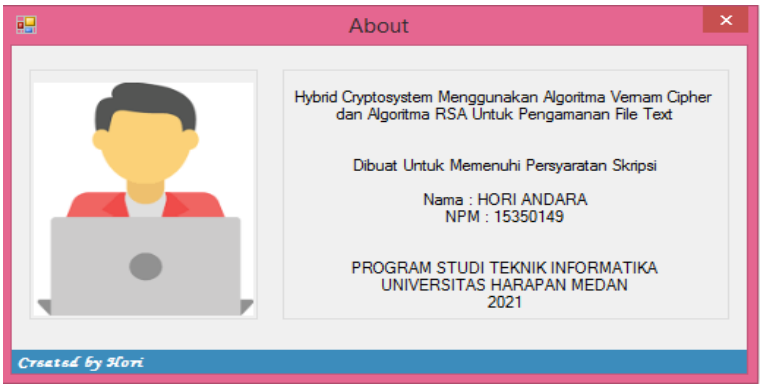
Pada *form help* atau bantuan ini merupakan penjelasan dari setiap *form* yang ada seperti pada *form* bangkit kunci, enkripsi dan dekripsi, tentang cara penggunaan pada system.



Gambar 6 Form *Help*

3.6 Tampilan Form About

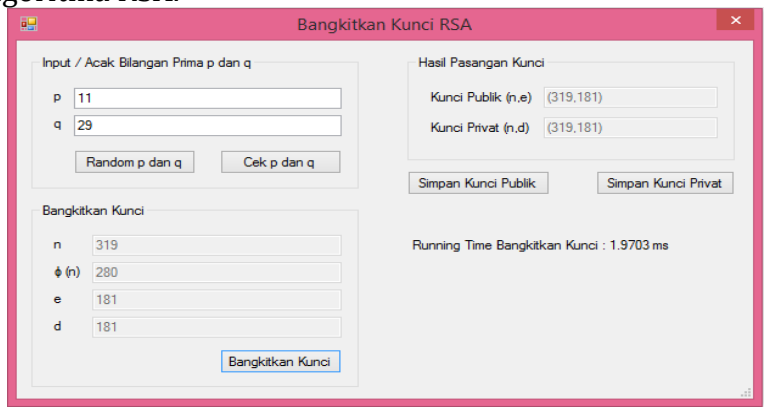
Pada *form about* ini merupakan *form* tambahan yang digunakan untuk menampilkan informasi profil yang mencakup nama dan judul aplikasi.



Gambar 7 Form *About*

3.7 Pengujian Pembangkit Kunci

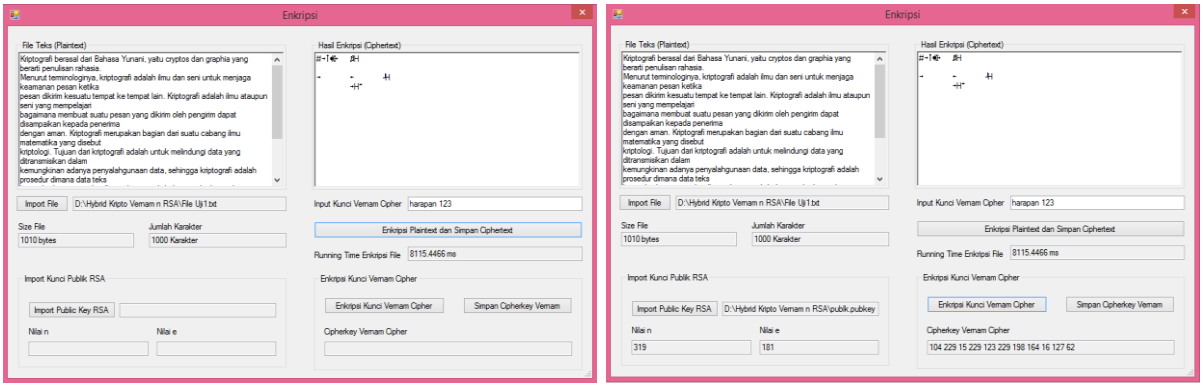
Pada pengujian ini dibuat sebuah skenario agar lebih mudah memahami proses bangkit kunci pada sistem. Kunci publik dan privat didapatkan saat proses bangkit kunci menggunakan algoritma RSA.



Gambar 8 Pengujian Sistem Bangkitkan Kunci

3.8 Pengujian Enkripsi *File* Teks dan Pengujian Enskripsi Kunci

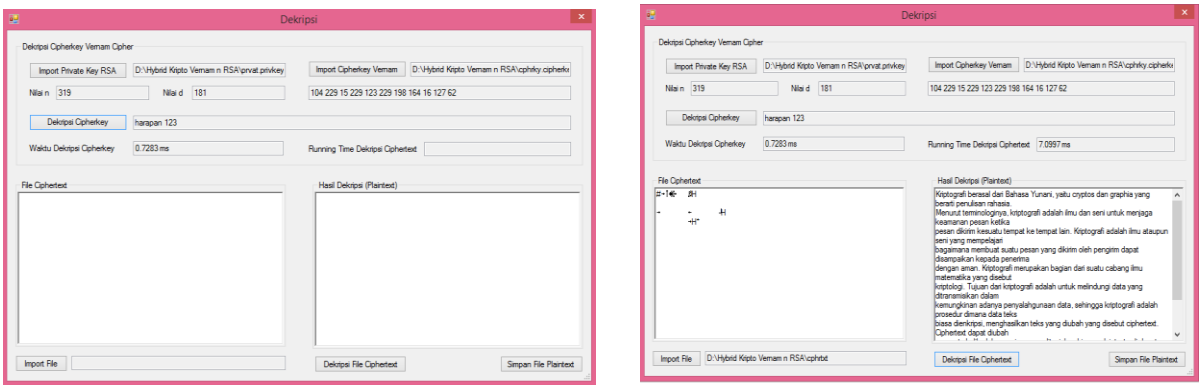
Pada proses enkripsi *file* teks yang bisa untuk dienkripsi hanya *file* yang memiliki *format***.txt*, selain dari *format* tersebut *file* tidak dapat di enkripsi dan Proses enkripsi ini kunci yang akan dikirim agar lebih aman kerahasiaanya. Untuk mengenkripsi kunci *Vernam Cipher* dengan menggunakan kunci publik RSA.



Gambar 9 dan Gambar 10 Menampilkan Pengujian Enskripsi *File* Teks dan Pengujian Enskripsi Kunci

3.9 Pengujian Deskripsi Kunci dan Pengujian Deskripsi *File* Teks

Proses dekripsi ini kunci yang akan dikirim agar lebih aman kerahasiaanya. Untuk mengenkripsi kunci *Vernam Cipher* dengan menggunakan kunci publik RSA dan Setelah melakukan proses dekripsi kunci menggunakan kunci private RSA, maka dapat melakukan dekripsi untuk pesan menggunkan kunci yang sudah di dekripsi.



Gambar 11 dan Gambar 12 Menampilkan Pengujian Deskripsi Kunci dan Pengujian Deskripsi *File* Teks

4. SIMPULAN

Kesimpulan yang dapat diambil setelah melakukan implementasi dan pengujian sistem terhadap pengaman *file* teks dengan menggunakan algoritma asimetris RSA dan algoritma simetris *Vernam Cipher* dalam skema *hybrid cryptosystem*, yaitu sebagai berikut:

1) Kombinasi algoritma asimetris RSA dan algoritma simetris *Vernam Cipher* dalam skema

hybrid cryptosystem berhasil diterapkan untuk pengamanan *file* teks berekstensi *.txt dengan cara mengenkripsi *file* dan mengembalikannya seperti semula dengan proses dekripsi tanpa ada perbedaan karakter dan ukuran pada *file*.

2) Hasil pengujian pada waktu proses enkripsi dan dekripsi diperoleh bahwa waktu proses algoritma berbanding lurus dengan panjang karakter *file* teks. Artinya semakin panjang *file* teks yang digunakan maka akan semakin lama juga waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi pada *file* teks tersebut.

DAFTAR PUSTAKA

[1] S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, and S. Srinjiwi, "Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 6, no. 1, pp. 1–10, 2019, doi: 10.33330/jurteksi.v6i1.395.

[2] S. Zamara, "Penerapan Algoritma Vegenere Cipher Dan Vernam Cipher Dalam Penggamanan File Text," *JURIKOM (Jurnal Ris. Komputer)*, vol. 6, no. 3, pp. 326–332, 2019, [Online]. Available: http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom/article/view/1345.

[3] P. S. Eka, "Implementasi Keamanan Data Menggunakan Algoritma Vernam Cipher Dan Playfair Cipher," *J. Pelita Inform.*, vol. 17, pp. 430–435, 2018.

[4] A. Ginting, R. R. Isnanto, and I. P. Windasari, "144706-ID-implementasi-algoritma-kriptografi-rsa-u," *J. Teknol. dan Sist. Komput.*, vol. 3, no. 2, pp. 253–258, 2015, [Online]. Available: https://media.neliti.com/media/publications/144706-ID-implementasi-algoritma-kriptografi-rsa-u.pdf.

[5] Diana. M & Zebua. T. 2018. Optimalisasi Beaufort Cipher Menggunakan Pembangkit Kunci RC4 Dalam Penyandian SMS. Jurnal Sains Komputer & Informatika (J- SAKTI), Vol. 2 No. 1.

[6] Legito. 2020. Penyandian Teks Dengan Kombinasi Vernam Cipher dan Caesar Cipher 220. Jurnal Mahajana Informasi, Vol. 5, No. 1.

[7] Rusmala & Prasti, D., 2019, Implementasi Metode Rail Fence Chiper dan Row Transposition Chiper Pada Mata Kuliah Kriptografi. Jurnal Ilmiah d'Computare Vol. 9, Edisi Januari.