ANALISIS PENINGKATAN HYBRID CRYPTOSYSTEM UNTUK ENKRIPSI DAN DEKRIPSI MENGGUNAKAN VIGENERE CIPHER DAN RSA PADA TEXT

AlfianYunianto Suseno [1], Nina Sulistiyowati [2], Purwantoro [3]
Program Studi Teknik Informatika,Universitas Singaperbangsa Karawang
alfianyunianto74@gmail.com [1],
nina.sulistio@unsika.ac.id [2], purwantoro.masbro@staff.unsika.ac.id [3]

Submitted July 30, 2021; Revised November 22, 2021; Accepted November26, 2021

Abstrak

Ilmu kriptografi merupakan suatu teknik matematis yang berhubungan dengan aspek keamanan. Ilmu kriptografi memiliki dua jenis teknik yang memiliki kelebihan dan kekurangannya sendiri. Untuk mengatasi masing-masing kekurangan kedua teknik tersebut dapat digunakan metodologi *hybrid cryptosystem.* Metodologi *hybrid cryptosystem* adalah sebuah metode untuk mengamankan suatu file atau informasi dengan menggunakan kombinasi antara algoritma simetris dan asimetris. Dengan penggabungan kedua teknik tersebut maka didapat sebuah algoritma yang kuat dan saling menutupi kekurangannya masing-masing. Tahapan yang dilakukan dalam penelitian ini adalah melakukan pembangkitan token acak dengan menggunakan *pseudorandom number generator*, lalu dengan token acak tersebut akan dilakukan pembangkitan tabel dan *key* acak, kemudian *plaintext* dienkripsi menggunakan tabel dan *key* acak tersebut, sedangkan token yang digunakan akan dienkripsi dengan RSA. Hasil penelitian yang ditampilkan adalah hasil analisa dari penelitian ini yaitu peningkatan varian bentuk *ciphertext* yang dihasilkan dan kemudahan dalam pembacaan hasil dekripsi karena penggunaan *printable ASCII* dalam proses enkripsi, dan hasil token yang dienkripsi memiliki panjang yang lebih pendek dan berbentuk hexadesimal.
Kata Kunci : Kriptografi, *Vigenere cipher,* RSA, *Hybrid cryptosystem*

Abstract

Cryptography is a mathematical technique related to security aspects. Cryptography has two techniques with their own advantage and disadvantage. The disadvantage of those techniques can be solved by using a hybrid cryptography method. The hybrid cryptosystem is a method for securing a file or information by using a combination of symmetric and asymmetric algorithms. By combining the two techniques, we can obtain a strong algorithm that cover each other disadvantage. Steps taken in this study are generating random token with pseudorandom number generator, then using the random token to generate random table and key, then the plaintext is encrypted with random table and key, meanwhile the token is encrypted using RSA. The shown results of this research are analytic results of this research, which are the improvement of ciphertext variant and the easiness of reading decryption result by using printable ASCII in the encryption and encrypted token with a shorter length and a hexadecimal form.
Keywords : *Cryptography, Vigenere cipher, RSA, Hybrid Cryptosystem*

1. PENDAHULUAN

Dalam pengiriman sebuah informasi baik yang tradisional maupun modern sangatlah penting dalam menjaga pesan tersebut tidak terbaca oleh orang yang tidak dikenal. Informasi akan tidak berguna lagi apabila di tengah proses pengiriman, informasi itu disadap atau dibajak oleh orang yang tidak berhak [1]. Untuk menjaga informasi tersebut tetap terjaga keamanannya maka perlu digunakannya ilmu kriptografi. kriptografi adalah suatu

ilmu atau keahlian teknik matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integritas data, dan autentikasi keaslian data [2]. Kriptografi memiliki fungsi dasar berupa enkripsi dimana proses mengubah pesan menjadi bentuk yang tidak terbaca dan dekripsi dimana proses mengubah pesan tidak terbaca dari hasil enkripsi menjadi dapat dibaca kembali. Ilmu kriptografi terdiri dari dua jenis, yaitu simetris dan asimetris. Kriptografi simetris berfokus pada pengamanan komunikasi antara pengirim dan penerima menggunakan kunci rahasia, sedangkan asimetris mengamankan komunikasi dengan *public key* dan *private key*. Dalam segi keamanan dalam melakukan enkripsi pesan, kriptografi asimetris lebih unggul karena panjang kunci yang digunakan lebih panjang dari pada kriptografi simetris yang mana membuat kriptografi simetris menjadi kurang aman untuk menyimpan data sensitif [3], tetapi kriptografi simetris memiliki kecepatan yang lebih baik karena proses enkripsi tidak serumit pada kriptografi asimetris

Pada 15 teknik kriptografi simetris dan asimetris diketahui 6 dari teknik kriptografi simetris tersebut rentan terhadap serangan *bruteforce*, sedangkan pada teknik kriptografi asimetris tersebut rentan terhadap serangan *cycle attack, man in the middle*, atau *side channel attack* [4]. Untuk mengatasi beberapa ancaman kelemahan pada masing-masing jenis kriptografi dapat dilakukan penggabungan kedua jenis kriptografi tersebut, penggabungan tersebut dapat dilakukan dengan menggunakan metodologi *hybrid cryptosystem*. Penggabungan kedua jenis kriptografi sebelumnya telah dilakukan dalam penelitian yang berjudul "*Hybrid Cryptosystem Analysis by Using The Combination of Vigenere Cipher and RSA for Text Security*" dengan menggabungkan *vigenere cipher* dengan RSA, tetapi pada penelitian tersebut masih ada kekurangan diantaranya jenis pesan yang digunakan terbatas pada huruf alfabet dan hasil dekripsi yang didapat adalah sekumpulan huruf alfabet kapital tanpa adanya pembatas sehingga masih sulit untuk dibaca [5].

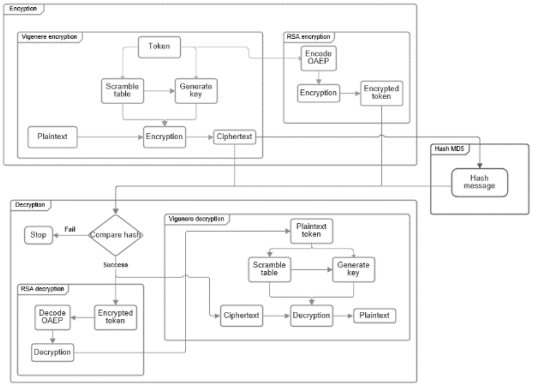
Telah dilakukan beberapa penelitian terkait teknik kriptografi yang digunakan pada penelitian tersebut untuk mengetahui apa yang bisa dilakukan untuk meningkatkan penelitian tersebut. Salah satunya adalah penelitian "*A Modified Version of Vigenere Cipher using 95 × 95 Table*" yang menggunakan tabel *vigenere* 95x95 untuk melakukan proses enkripsi [6]. Dengan penggunaan tabel tersebut maka masalah pada penelitian sebelumnya dapat teratasi. Penelitian ini bertujuan untuk melakukan analisis terhadap peningkatan *hybrid cryptosystem* pada penelitian sebelumnya. Analisis yang dilakukan adalah bagaimana hasil enkripsi yang dilakukan setelah dilakukan peningkatan dan berapa lama waktu yang dibutuhkan dalam melakukan proses tersebut.

2. METODE PENELITIAN

Penelitian yang dilakukan adalah analisis peningkatan penelitian penggabungan algoritma kriptografi *vigenere cipher* dengan RSA menggunakan metodologi *hybrid cryptosystem*. Akan dilakukan simulasi proses enkripsi dan dekripsi dari algoritma tersebut, kemudian dilakukan pengujian perhitungan kecepatan yang dibutuhkan untuk *plaintext* dapat dienkripsi dan didekripsi kembali, kemudian dilakukan pembandingan hasil *ciphertext* dan lama waktu proses dengan penelitian [4] yang dibahas pada bagian hasil dan pembahasan. Tahapan yang dilakukan terdiri dari 5 tahap, yaitu:

a. Pembangkitan token
b. Enkripsi
c. Autentikasi Pesan
d. Dekripsi
e. Dokumentasi

Pada proses enkripsi dan dekripsi akan digunakan alur sesuai pada **Gambar 1**.



Gambar 1. Alur Enkripsi dan Dekripsi

Dari alur pada **Gambar 1** dapat terlihat beberapa langkah yang harus dilakukan, langkah tersebut diantaranya:

a. Enkripsi dengan vigenere cipher
Vigenere cipher adalah teknik kriptografi klasik yang lebih aman dari pada *caesar cipher* [7]. *Vigenere cipher* merupakan bagian dari penyandian polialfabetik yang menggunakan tabel substitusi susunan alfabet 26x26 yang disusun secara horizontal dan vertical. Pada penelitian ini akan dilakukan proses enkripsi dengan menggunakan tabel modifikasi 95x95 seperti pada penelitian [5] yang berisi *printable ASCII*, kemudian dilakukan pengacakan urutan menggunakan token acak dan *pseudorandom number generator*. Dengan penggunaan tabel modifikasi maka rumus perhitungan yang digunakan akan berubah menjadi pada rumus (1).

$$Ci = (Pi + Ki) \bmod 95 \quad (1)$$

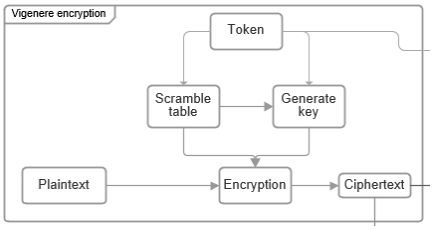
Keterangan:

Ci = *cipher index*

Pi = *plaintext index*

Ki = *key index*

Proses enkripsi *plaintext* tersebut menghasilkan *ciphertext*, *ciphertext* tersebut kemudian diambil nilai hash nya dengan MD5 untuk proses autentikasi nantinya. Sehingga pada proses ini akan menghasil *ciphertext* dan *ciphertext hash*.

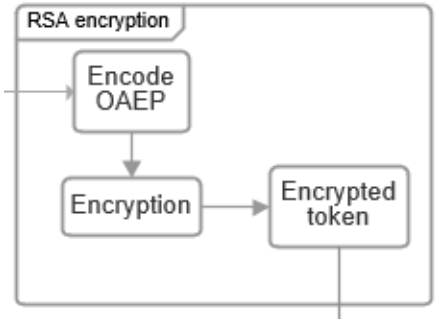


Gambar 2. Enkripsi *Plaintext* dengan *Vigenere Cipher*

b. Enkripsi dengan RSA
RSA adalah teknik algoritma asimetris yang biasa digunakan untuk melindungi data dimana *confidentiality* adalah poin yang krusial dan sangat penting. Keamanan pada RSA ada pada *integer* masalah faktorisasi sebuah angka besar gabungan dan sebuah gabungan angka untuk bilangan prima dengan akar modulus [8]. Dalam penggunaannya, RSA biasanya digunakan bersamaan dengan teknik *padding*. Pada penelitian ini akan digunakan penggunaan RSA dengan *padding* OAEP dengan tujuan untuk peningkatan keamanan dan kecepatan proses enkripsi. OAEP sendiri adalah skema *padding* yang biasa digunakan bersamaan dengan RSA dan terstandarisasi didalam PKCS#1 v2, penggunaan *padding* tersebut pada RSA biasa disebut RSA-OAEP [9]. Proses enkripsi token dilakukan dengan melakukan *padding* terlebih dahulu pada token sehingga didapat nilai *padded token*, kemudian dilanjutkan ke proses enkripsi menggunakan RSA. Jumlah bit yang digunakan pada RSA tersebut adalah 1024 bit dengan rumus perhitungan yang digunakan terlihat pada rumus (2).

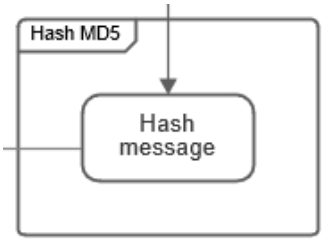
$$C = m^{e} \bmod n \quad (2)$$

Proses enkripsi tersebut menghasilkan *encrypted token* yang akan dikirimkan bersamaan dengan *ciphertext* dan *ciphertext hash* agar proses dekripsi dapat dilakukan.



Gambar 3. Enkripsi Token dengan RSA

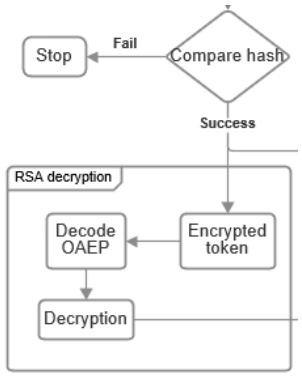
c. Autentikasi pesan
Sebelum proses dekripsi dilakukan, diperlukan adanya pengecekan hash pada *ciphertext* untuk mengetahui apakah pesan telah mengalami perubahan atau tidak. Terdapat berbagai macam hash yang dapat digunakan untuk melakukan proses autentikasi tersebut, tetapi pada penelitian ini akan digunakan MD5 hash karena proses hash yang cepat. MD5 adalah salah satu dari banyaknya fungsi hash yang ada saat ini. Fungsi hash sendiri adalah algoritma satu arah yang mengambil panjang variabel sebagai *input* dan memproduksi *string* dengan panjang yang telah ditetapkan sebagai *output* [10]. Proses perbandingan dilakukan dengan membandingkan *ciphertext hash* dengan *ciphertext* yang telah di hash pada tahap ini. Jika terdeteksi adanya perubahan maka proses dihentikan, sedangkan jika tidak terdeteksi adanya perubahan maka proses dekripsi dapat dilakukan.



Gambar 4. *Hash Ciphertext*

d. Dekripsi dengan RSA
Encrypted token didekripsi dengan RSA menggunakan rumus (3). Setelah proses dekripsi dilakukan selanjutnya dilakukan proses *decode* OAEP hingga didapatkan *decrypted token* yang kemudian digunakan pada proses dekripsi *ciphertext*.

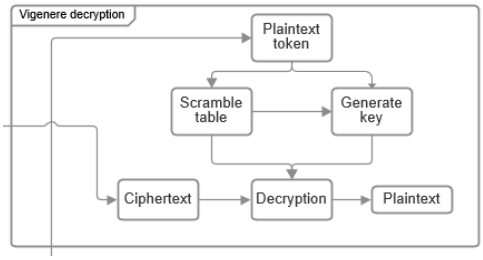
$$P = C^{d} \bmod n \quad (3)$$



Gambar 5. Dekripsi Token dengan RSA

e. Dekripsi dengan *vigenere cipher*
Proses terakhir yang dilakukan adalah proses dekripsi *ciphertext*. Rumus yang digunakan dalam proses dekripsi tersebut dapat dilihat pada rumus (4). Setelah proses dekripsi dilakukan maka didapat sebuah pesan *plaintext* yang sama dengan pesan yang digunakan sebelumnya.

$$Pi = (Ci + Ki) \bmod 95 \quad (4)$$



Gambar 6. Dekripsi *Ciphertext* dengan *Vigenere Cipher*

3. HASIL DAN PEMBAHASAN

Hasil dari penelitian yang dilakukan akan berupa perbandingan bentuk dan lama waktu proses enkripsi dan dekripsi dengan penelitian yang telah dilakukan sebelumnya. Perbandingan akan dilakukan dengan melakukan proses enkripsi dan dekripsi menggunakan penelitian saat ini dan penelitian [4] yang kemudian akan dibandingkan antara keduanya bentuk hasil enkripsi dan dekripsi, serta lama waktu yang dibutuhkan dalam prosesnya dengan menggunakan *plaintext* sepanjang 317 karakter sebagai bahan percobaan. *Plaintext* yang digunakan adalah "*In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information.*"

A. Perbandingan Hasil Enkripsi dan Dekripsi

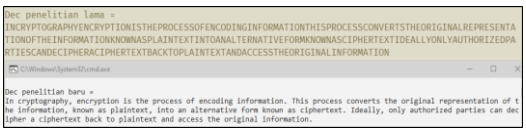
Pada penelitian saat ini didapat hasil enkripsi *plaintext* berupa sekumpulan *printable ASCII* sepanjang jumlah karakter *plaintext*, sedangkan pada penelitian [4] hanya berupa sekumpulan alfabet kapital dengan jumlah karakter tidak sepanjang *plaintext* karena pada proses enkripsinya diperlukan penghilangan karakter yang tidak digunakan seperti karakter spasi, tanda baca, dan lain-lain.

Gambar 7. Perbandingan Hasil Enkripsi *Plaintext*

Hasil enkripsi token yang digunakan juga terlihat adanya perbedaan. Pada penelitian saat ini akan didapat nilai enkripsi token berbentuk hexadesimal dengan panjang 128 bit, sedangkan pada penelitian [4] akan didapat hasil enkripsi berbentuk angka yang sangat panjang.

Gambar 8. Perbandingan Hasil Enkripsi Token

Dan pada proses dekripsi akan ditemukan perbedaan pada hasil yang didapat. Pada penelitian saat ini akan didapat hasil *plaintext* yang sama dengan sebelum dilakukannya enkripsi, sedangkan pada penelitian [4] akan didapat hasil sekumpulan alfabet kapital tanpa adanya tanda pemisah.

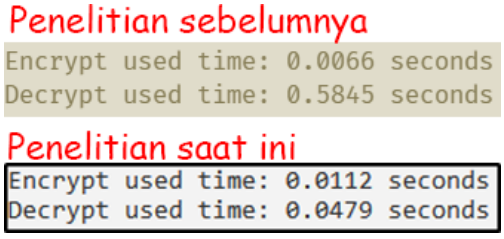


Gambar 9. Perbandingan Hasil Dekripsi P*laintext*

B. Perbandingan Kecepatan Proses

Dengan melakukan proses enkripsi dan dekripsi pada kedua penelitian menggunakan *plaintext* dengan panjang 317 karakter, didapatkan hasil pada penelitian [4] membutuhkan waktu proses enkripsi 6,6 ms dan proses dekripsi membutuhkan waktu

584,5 ms. Sedangkan pada penelitian saat ini pada proses enkripsi membutuhkan waktu 11,2 ms dan proses dekripsi membutuhkan waktu 47,9 ms. Terlihat pada proses enkripsi, penelitian [4] lebih cepat dibanding penelitian saat ini tapi pada proses dekripsi penelitian saat ini jauh lebih cepat, jika dihitung total waktu yang dibutuhkan maka penelitian [4] membutuhkan waktu 591,1 ms untuk menyelesaikan proses enkripsi dan dekripsi, sedangkan pada penelitian saat ini membutuhkan waktu 59,1 ms, dapat dikatakan penelitian saat ini lebih cepat dalam memproses enkripsi dan dekripsi dari pada penelitian [4]. Perbedaan waktu tersebut terjadi karena pada penelitian ini digunakan tabel modifikasi berjumlah 95x95, dengan penambahan jumlah tabel tersebut maka akan didapat peningkatan lama waktu proses yang dilakukan, selain itu penggunaan *padding* OAEP juga membantu mempersingkat proses enkripsi token yang digunakan karena *padding* yang dilakukan dapat menghasilkan sebuah urutan angka desimal sehingga tidak perlu mengubah satu persatu karakter menjadi kode *ASCII* untuk dapat dienkripsi menggunakan RSA.



Gambar 10. Perbandingan Lama Waktu Proses

4. SIMPULAN

Berdasarkan penelitian yang telah dilakukan, penelitian saat ini memiliki hasil berupa peningkatan yang lebih baik dari pada penelitian sebelumnya. Peningkatan pada kecepatan dipengaruhi pada proses enkripsi token yang dilakukan, dimana sebelumnya dilakukan proses enkripsi pada tiap karakter yang telah diubah kedalam bentuk kode *ASCII* menggunakan RSA yang menyebabkan hasil enkripsi menjadi sangat panjang karena berisi nilai hasil enkripsi per karakter dan membuat proses dekripsi lebih memakan waktu. Sedangkan pada penelitian saat ini digunakan proses *padding* terlebih dahulu menggunakan OAEP dengan hasil *padding* yaitu berbentuk hexadesimal yang dapat diubah ke bentuk binary, dengan mengubah ke bentuk binary maka dapat dilakukan proses enkripsi RSA sebanyak satu kali sehingga tidak terlalu membebani saat proses dekripsi. Hasil dekripsi yang didapat juga lebih mudah dibaca karena pada penelitian saat ini telah digunakan tabel 95x95 yang mengandung karakter special seperti spasi dan tanda baca lainnya dengan kekurangannya adalah proses enkripsi yang dilakukan lebih lama dari penelitian sebelumnya.

DAFTAR PUSTAKA

[1] M. D. Irawan, “Implementasi Kriptografi Vigenere Cipher Dengan Php,” *Jurnal Teknologi Informasi*, vol. 1, no. 1, p. 11, 2017, doi: 10.36294/jurti.v1i1.21.

[2] R. N. Ibrahim, “Perangkat Lunak Keamanan Data Menggunakan Algoritma Kriptografi Simetri Tiny Encription Algorithm (TEA)” vol. 13, no. 1, pp. 1–10, 2019.

[3] F. Maqsood, M. Ahmed, M. Mumtaz, and M. Ali, “Cryptography: A Comparative Analysis for Modern Techniques,” *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, pp. 442–448, 2017, doi: 10.14569/ijacsa.2017.080659.

[4] M. A. Al-Shabi, "A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 9, no. 3, p. p8779, 2019, doi: 10.29322/ijsrp.9.03.2019.p8779.

[5] R. Jamaludin, "Hybrid Cryptosystem Analysis by Using The Combination of Vigenere Cipher and RSA for Text Security," vol. 1, no. 1, pp. 89–100, 2020, doi: 10.31098/ic-smart.v1i1.31.

[6] K. Nahar and P. Chakraborty, "A Modified Version of Vigenere Cipher using 95×95 Table," *International Journal of Engineering and Advanced Technology*, vol. 9, no. 5, pp. 1144–1148, 2020, doi: 10.35940/ijeat.e9941.069520.

[7] I. Saputra, Mesran, N. A. Hasibuan, and R. Rahim, "Vigenere Cipher Algorithm with Grayscale Image Key Generator for Secure Text File," *International Journal of Engineering Research & Technology (IJERT)*, vol. 6, no. 01, pp. 266–269, 2017.

[8] M. M. Hoobi, S. S. Sulaiman, and I. A. Abdulmunem, "Enhanced Multistage RSA Encryption Model," *IOP Conference Series: Materials Science and Engineering*, vol. 928, no. 3, 2020, doi: 10.1088/1757-899X/928/3/032068.

[9] E. Kiltz, A. O'Neill, and A. Smith, "Instantiability of RSA-OAEP Under Chosen-Plaintext Attack," *Journal of Cryptology*, vol. 30, no. 3, pp. 889–919, 2017, doi: 10.1007/s00145-016-9238-4.

[10] D. Rachmawati, J. T. Tarigan, and A. B. C. Ginting, "A comparative study of Message Digest 5(MD5) and SHA256 algorithm," *Journal of Physics: Conference Series*, vol. 978, no. 1, 2018, doi: 10.1088/1742-6596/978/1/012116.