Implementasi Multi Enkripsi Menggunakan Algoritma Vigenere Cipher dan RSA untuk Pengamanan Informasi dan Data

I Gusti Ngurah Made[1], Gusti Eka Yuliastuti[2], Citra Nurina Prabiantissa[3]
Institut Teknologi Adhi Tama Surabaya[1,2,3]
e-mail: igustimade.dwi@gmail.com

ABSTRACT

Data security is a top priority in various fields and covers all levels of their respective fields. One method for protecting data is through encryption, although obstacles often occur, such as long execution durations and significant resource usage, especially in strong encryption methods. To overcome this problem, the author innovated by combining two encryption methods, namely Vigenere Cipher and RSA. In the Vigenere Cipher method, data were randomized using a key, which was repeated and then processed again using the RSA method. It relies on mathematical principles in carrying out data scrambling operations, thereby increasing the complexity and security of encryption. The results of the Avalanche Effect test produced an average value of above 90%, indicating that the multi-encryption application developed by the author had a relatively strong level of security even with a relatively short execution time. This multi-encryption implementation had been applied to a MySQL database containing patient medical record data from 20 patients and was successfully executed without any problems.
Keywords*: Multi encryption, RSA, Vigenere Cipher*

ABSTRAK

Keamanan data merupakan prioritas utama dalam berbagai bidang serta meliputi semua tingkatan dari bidangnya masing-masing. Salah satu metode dalam melindungi data adalah melalui enkripsi, walaupun sering kali ditemui kendala seperti durasi eksekusi yang lama dan penggunaan sumber daya yang signifikan khususnya dalam metode enkripsi kuat. Untuk mengatasi permasalahan ini penulis mencoba melakukan inovasi dengan memadukan dua metode enkripsi yaitu *Vigenere Cipher* dan RSA. Pada metode *Vigenere Cipher* data akan diacak menggunakan kunci yang diulang-ulang kemudian diproses lagi menggunakan metode RSA yang mengandalkan prinsip-prinsip matematika dalam melakukan operasi pengacakan data sehingga meningkatkan kompleksitas dan keamanan enkripsi. Pengujian metode ini dibuktikan melalui pengujian *Avalanche Effect* yang menghasilkan nilai rata-rata di atas 90% dimana ini menunjukkan bahwa penerapan *multi* enkripsi yang dikembangkan penulis memiliki tingkat keamanan yang tergolong kuat meski dengan waktu eksekusi yang relatif singkat. Implementasi *multi* enkripsi ini telah diaplikasikan pada database MySQL yang berisi data rekam medis pasien dari 20 data pasien dan berhasil dijalankan tanpa adanya kendala sedikitpun.

Kata kunci : Multi enkripsi, RSA, *Vigenere Cipher*

PENDAHULUAN

Menjaga kerahasiaan data adalah salah satu faktor yang sangat penting dalam sistem pengiriman informasi. Hal ini terkait dengan pentingnya informasi tersebut sampai ke tangan orang-orang yang memiliki kepentingan terhadapnya. Jika informasi disadap atau dibajak oleh orang yang tidak berhak selama proses pengiriman, maka informasi tersebut tidak akan berguna lagi[1]. Pencurian informasi dapat dicegah dengan berbagai cara, salah satunya adalah dengan menggunakan kriptografi.

Kriptografi pada awalnya dicantumkan sebagai ilustrasi yang menunjukkan cara sembunyikan pesan. Namun, dalam konteks kriptografi modern, ilmu yang berbasis teknologi matematika adalah ilmu yang digunakan untuk menggabungkan informasi seperti kerahasiaan data dan analisis entitas. Kriptografi modern tidak hanya dicirikan oleh penggunaan data pribadi tetapi juga oleh penggunaan teknologi yang menyediakan informasi[2].

TINJAUAN PUSTAKA

Implementasi Enkripsi

Adapun implementasi yang diterapkan pada kombinasi dua metode enkripsi yaitu *vigenere cipher* dan RSA yaitu dengan menerapkan kombinasi kedua enkripsi tersebut kedalam enkripsi database dimana value data yang nantinya akan dimasukkan kedalam database akan dienkripsi terlebih dahulu sehingga nantinya pada saat data tersebut berada didalam database sudah dalam keadaan terenkripsi[3].

Enkripsi Vigenere Cipher

Sandi *vigenere cipher* adalah jenis sandi yang menggunakan alfabet majemuk. *Vigenere Cipher* merupakan metode enkripsi teks dengan Menggunakan *cipher Caesar* dan kunci yang ditentukan, *Vigenere Cipher* mengenkripsi teks. Ini adalah varian dari algoritma kriptografi standar, yang dibedakan oleh dasar matematikanya. Selain itu, *Vigenere Cipher* dapat mengenkripsi dan mendekripsi ciphertext menggunakan tabel *Vigenere*[4]. Tabel *Vigenere* ini digunakan untuk menampilkan *ciphertext* untuk kunci yang dipilih saat ini. Jika panjang kunci lebih jauh dari *plainext*, kunci tersebut akan terus memproses data dari waktu ke waktu.

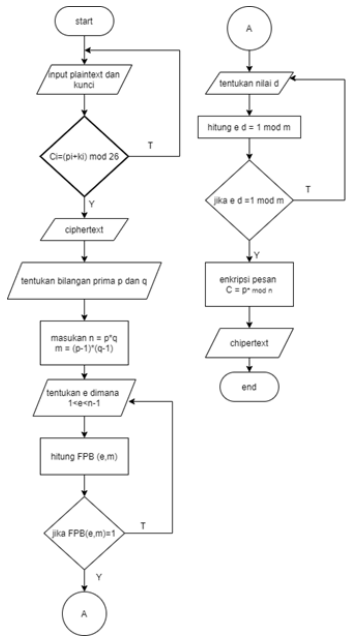
Enkripsi RSA

Sandi *RSA* merupakan algoritma kriptografi kunci publik(asimetris)[5]. *RSA* adalah salah satu *Cryptosystem* Kunci Publik yang umum digunakan untuk memastikan kerahasiaan data digital. Keamanan proses enkripsi dan dekripsi pada model ini bertumpu pada sulitnya memfaktorkan modulus n yang sangat besar[6].

METODE

Multi Enkripsi

Pada gambar 1 berikut ini ditunjukkan flowchart dari proses multi enkripsi dari penggabungan *vigenere cipher* dengan RSA:



Gambar 1. Contoh Flowchart multi enkripsi

Berikut adalah algoritma enkripsi dari metode multi enkripsi:

1. Masukan *plaintext dan* kunci
2. Masukan kunci
3. Hasil *plaintext* dan kunci akan dijadikan ASCII
4. Melakukan XOR antara plainteks ASCII dengan kunci
5. Hasil XOR dienkripsikan menjadi chiperteks
6. Hasil chiperteks dan membuat pasangan kunci publik dan privat
7. Kunci publik digunakan melakukan enkripsi
8. Selesai

HASIL DAN PEMBAHASAN

Pembahasan Data I

Pengujian Avalanche Effect merupakan suatu pengujian yang dilakukan dengan cara membandingkan perubahan bit yang terjadi antara sebuah input dan output dari sebuah algoritma enkripsi. Tujuan dari pengujian ini adalah apabila suatu metode enkripsi atau fungsi hash kriptografi tidak memiliki nilai Avalanche Effect pada tingkat/batasan minimal yang sudah ditentukan, maka dapat disimpulkan bahwa metode enkripsi tersebut memiliki pengacakan yang buruk, sehingga seorang kriptanalis dapat membuat prediksi mengenai input dari suatu ciphertext.

Tabel 1. Data layout artikel SNTEKPAN

No	Nama Pasien	Plaintext	Panjang bit
1	Budi Hartono	Tegalsari	9
2	Ayu Lestari	Genteng	7

no	plaintext	Chipertext	Presentase avalanche effect (%)
1	Tegalsari	qFg2N+4+8LFLK0C1zQwajOQB608oc4dYT0mJFaziC4COiW4JLdYGPt+0/gA4oTnnbKfnxzOpJXjmbecuS/X1Y4iyZJ65MufLdeHAtI8fXAFOm1CwMpqGa4Oi0t3PSmsYm7U+qeBFH890y24JXtAItFUJ2iucOSSbW3eDBzlOwP82go64E/vverDCI0zi0GIKfxDh5afVnfHYV9ytLttsjhRrgtDA1rqLbc0qOglf6/wZ53nofVdhW644iQ2mVr1yGB7QO8beV2iNscWXA06F5zh65jWqH12cROKg4LDAixu9rosA7ITFc5sfg/C2LDsdliiILSu+aIlYZZmRQo/ebA==	98.33%
2	Genteng	CU5SPcRjOlZ1gzrzi+THJDcCIl5BwvXxLVOKY+WvYIh9zTUAvcWwwIGm+QDvATR5FUepGFcanndQ8es44uD4UYknPuX95/crJ5bMnjGsDbSAHZgRbfezmlqzd2eTNBghsnXpvHRfUaxg+GUfFdnmBRjSMn7Wnxyz2hGQkba91og9y57xJtZyPflOopr6YAOMlusFDedZvaQHNe5wZ2rVdGhE/IIRKMgnBfIV+jGOpdVMAMlE+ryRGNBndXosUW3ENyyMh/hCqaQE1vFkIMu+QSGlPZ0zhjBF5g+CT7oDtopc4ixAd4m78Hm3DYbGImoPqxxlmne2Hy577iHxU9UXKw==	98.80%
Rata – rata			98.56%

KESIMPULAN

Berdasarkan penelitian dan praktek uji coba yang telah dilakukan, dapat diambil beberapa kesimpulan sebagai berikut ini:

1. Kombinasi enkripsi antara *vigenere cipher* dengan RSA menghasilkan enkripsi yang tergolong kuat hal ini dapat dibuktikan dari nilai rata – rata pengujian avalanche effect menyentuh angka 98.56%
2. Kombinasi metode enkripsi *vigenere cipher* dan RSA menghasilkan *ciphertext* acak dengan panjang 2752 bit yang berarti lebih sulit bagi penyerang untuk mengidentifikasi pola atau mencari kelemahan dalam algoritma enkripsi karena teks menjadi lebih kompleks dan sulit untuk dianalisis.

DAFTAR PUSTAKA

[1] “Irawan - 2017 - IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER DENGAN PH.pdf.”

[2] "Karman and Nurhasan - 2019 - PERANCANGAN SISTEM KEAMANAN DATA INVENTORY BARANG .pdf."
[3] S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, and S. Srinjiwi, "ANALISIS PERFORMA KRIPTOGRAFI HYBRID ALGORITMA BLOWFISH DAN ALGORITMA RSA," *JURTEKSI J. Teknol. Dan Sist. Inf.*, vol. 6, no. 1, pp. 1–10, Dec. 2019, doi: 10.33330/jurteksi.v6i1.395.
[4] "Abdullah - 2017 - Volume 1 Nomor 1 November 2017.pdf."
[5] "Teknik Informatika Universitas Khairun and Mubarak - 2019 - RANCANG BANGUN APLIKASI WEB SEKOLAH MENGGUNAKAN UM.pdf."
[6] "Warnilah and Nugraha - 2018 - Komparasi Algoritma Kriptografi Elgamal Dan Caesar.pdf."