# Simulasi Kriptografi Pesan Teks Menggunakan Vigenere Cipher Dan Rc4

***Cryptographic Simulation of Text Messages Using Vigenere Cipher and Rc4***

Ismail Budiman1, Arita Wintanti2

1Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Mercu Buana Yogyakarta Jalan Jembatan Merah No.84C, Condongcatur, Depok, Soropadan, Condongcatur, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55281

Email: ismailbudiman6@gmail.com, arita@mercubuana-yogya.ac.id

 Tanggal submisi: ; Tanggal penerimaan:

# ABSTRAK

**Keamanan data adalah suatu hal yang diinginkan semua orang untuk menjaga privasi dengan menyembunyikan data. Sebuah data atau pesan yang bersifat rahasia harus benar-benar dijaga. Salah satu algoritma yang digunakan untuk pengamanan data yaitu kriptografi. Metode yang diterapkan untuk pengamanan ini adalah *vigenere cipher* dan RC4. Kerahasiaan dan keaslian dokumen merupakan salah satu aspek penting sehingga jika kerahasiaan dan keaslian dokumen dirusak oleh pihak yang tidak bertanggung jawab maka informasi sudah tidak berguna lagi. Maka dibuatlah aplikasi enkripsi teks dengan menerapkan algoritma *vigenere cipher* dan RC4. Penerapan algoritma *vigenere Cipher* dan RC4 adalah untuk meningkatkan tingkat keamanan dari proses enkripsi. Berdasarkan hasil penelitian terdapat 30 data yang diuji berhasil dienkripsi.**

**Kata kunci**: Kriptografi, RC4 dan Vigenere Cipher.

ABSTRACT

***Data security is something that everyone wants to maintain privacy by hiding data. A data or message that is confidential must be strictly guarded. One algorithm used for data security is cryptography. The method applied for this security is vigenere cipher and RC4. The confidentiality and authenticity of documents is one important aspect so that if the confidentiality and authenticity of documents are damaged by irresponsible parties, the information is no longer useful. So a text encryption application was made by applying the vigenere cipher and RC4 algorithm. The application of Vigenere Cipher and RC4 algorithms is to increase the security level of the encryption process. Based on the results of the study there were 30 data that were tested successfully encrypted.***

**Keywords**: *Cryptography, RC4 and Vigenere Cipher.*

# 1. PENDAHULUAN

Keamanan data adalah suatu hal yang diinginkan semua orang untuk menjaga privasi dengan menyembunyikan data. Sebuah data atau pesan yang bersifat rahasia harus benar-benar dijaga. Kriptografi adalah salah satu teknik untuk pengamanan data atau pesan. Enkripsi dan dekripsi banyak digunakan untuk pengamanan data*.*

Salah satu algoritma kriptografi adalah *vigenere chiper* dan *RC4*. Algoritma *vigenere chiper* dan *RC4* termasuk kriptografi klasik yang menggunakan plainteks, cipherteks dan kunci untuk melakukan proses enkripsi dan dekripsi dalam pengamanan data. Vigenere cipher adalah salah satu jenis kriptografi simteris dan dikategorikan pula sebagai *polyalfabet cipher*. *RC4* adalah salah satu jenis *stream cipher* yang sinkron yaitu cipher yang memiliki kunci simetris dan mengenkripsi atau mendekripsi plainteks secara digit per digit atau bit per bit dengan cara mengkombinasikan secara operasi biner.

Penerapan algoritma *vigenere chiper* ternyata dapat dipecahkan oleh *crypanalyst* melalui metode kasiski. Metode kaisiski sebenarnya digunakan untuk mengestimasi kemungkinan panjang kunci yang muncul. Dengan melihat hal tersebuh penulis mencoba melakukan kombinasi enkripsi menggunakan algoritma Rivest Block *4* untuk meningkatkan keamanan sebuah pesan text.

# 2. TINJAUAN PUSTAKA

Penelitian dengan judul **“Implementasi Algoritma Kriptografi RC4 Dan Vigenere Cipher Pada Citra Bitmap”**. Objek citra digital yang digunakan adalah file bitmap. Citra tersebut diproses dengan melakukan enkripsi pada setiap pikselnya menggunakan algoritma RC4 kemudian dilanjutkan dengan menggunakan algoritma Vigenere Cipher. (Amirudin, 2016)

Melalui penelitian yang berjudul **“Enkripsi Dan Dekripsi Gambar Dengan Menggunakan Perpaduan Algoritma Base64 Dan RC4”**. Mengekripsi sebuah gambar atau citra dan diubah kedalam bentuk teks yang mempunyai jumlah karakter yang besar sehingga jika file gambar dienkripsi dengan mengenkripsi perkarakter harus menggunakan metode algoritma yang cepat dalam melakukan prosesnya. Dalam proses pengenkripsiannya sistem ini menggunakan algoritma RC4 dan di kombinasikan dengan algoritma Base64 karna adanya perbedaan pembacaan HTML dan File, maka saat melakukan deskripsi file yang berubah seusai penulisan HTML yang mengakibatkan file asli atau plainteksnya tidak sama dengan hasil deskripsi.(Putra & Hayati, 2018)

Penelitian dengan judul **“Implementasi Kriptografi Vigenere Cipher Pada Media Teks Dengan Kombinasi Transposisi Kolom”.** Penelitian ini dilakukan untuk penyelesaian kasus pengamanan pada media teks. Pada penelitian ini digunakan media teks sebagai implementasi kriptografi menggunakan algoritma vegenere chiper dengan kombinasi algoritma transposisi kolom. Penelitian ini membuktikan bahwa pesan asli (Plaintext) dapat di proses enkripsi dengan baik menggunakan kombinasi algoritma tersebut serta dapat dikembalikan seperti semula. Selain itu penelitian ini juga membuktikan apabila salah satu karakter dari teks tersebut diubah, maka akan mengubah semua karakter pada pesan dengan menggunakan avalanche effect dengan 5 (lima) buah percobaan mendapatkan nilai tertinggi 45,416. Salah satu komponen dalam avalanche effect adalah bit flipping atau dapat disebut juga perubahan bit dalam suatu proses enkripsi. Dalam bit flipping ini digunakan untuk menentukan perubahan bit sebelum dan sesudah proses enkripsi berjalan sehingga mempengaruhi dapat meningkatkan proses keamanan dalam proses kriptografi tersebut. (Sinaga & Umam, 2018)

Penelitian dengan judul **“Implementasi Algoritma RC4 Dan Playfair Cipher Untuk Mengamankan Data Teks”**. Penelitian ini dilakukan untuk menyelesaikan kasus pengamanan pada data teks. Pada penelitian ini digunakan media berupa data teks untuk mengimplemntasikan algoritma RC4 dan playfair cipher untuk mengamankan data teks. Data teks dapat berbentuk kata, surat, narasi dan berbagai bentuk lainnya. Oleh karena itu data teks dapat menjadi hal yang penting apabila data teks tersebut memiliki informasi yang berharga dan bersifat pribadi. Penggunaan metode ini dikarenakan algoritma ini menawarkan kesederhanaan dalam mengatasi data teks. Penyandian algoritma Ron’s Code 4 (RC4) merupakan algoritma modern dan salah satu algoritma kunci semetrik yang dibuat oleh RSA Data Security Inc (RSADSI) yang berbentuk stream cipher. RC4 menggunakan panjang kunci dari 1 sampai 256byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 byte. . (Simamora, 2017)

Penelitian dengan judul **“Implementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks Berbasis Android”**. Penelitian ini bertujuan untuk mengimplementasi dua algoritma kriptografi yaitu Rivest shamir dengan Playfair cipher. Pada penelitian ini menggunakan data text sebagai medianya. Tujuan dari penelitian adalah dengan dua algoritma yang ada diharapkan dapat lebih menjaga kemaanan pesan yang dikirim maupun diterima dengan mengubah terlebih dahulu kunci publik aslinya menggunakan playfair chiper setelah itu dipecahkan kembali menggunakan algoritma Rivest Shamir Adleman (RSA) sehingga menjadi pesan asli. (Kurniawan, Dedih, & Supriyadi, 2017).

**Kriptografi**

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. (Pabokory, Astuti, & Kridalaksana, 2015)

**Enkripsi**

Enkripsi adalah proses atau mekanisme untuk mengubah sebuah pesan dari yang dapat dimengerti menjadi pesan yang tidak dapat dimengerti dengan sebuah kode/metode tertentu.

**Vigenere cipher**

*Vigenere cipher* adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986 [7]. Algoritma Enkripsinya , sedangkan untuk deskripsinya . Untuk atau untuk .

***Rivest Code* 4**

*Rivest Code* 4 adalah cipher aliran yang digunakan secara luas pada sistem keamanan seperti protokol *Secure Socket Layer* (SSL). Algoritma kriptografi ini sederhana dan mudah diimplementasikan.

*Key Scheduling* digunakan untuk menginisialisasikan permutasi di array S panjang kunci didefinisikan sebagai jumlah byte di kunci dan mempunyai rentang panjang kunci dari 1 sampai 256. Khususnya antara 5-16 tergantung dari panjang kunci 40-128bit. Berikut adalah langkah langkah algoritma KSA [8]:

1. Nilai S diisi dengan nilai sesuai indeks:
2. Lakukan inisialisasi suatu nilai (j = 0 dan i = 0) kemudian lakukan perhitungan nilai j yang baru.
3. Kemudian tukarkan nilai S[i] dengan S[j] atau *swaping*.
4. Lakukan langkah kedua dan ketiga untuk setiap nilai i = 0, i = 1, i = 255, sebanyak 256 agar terbentuk kunci yang acak.

Tahap selanjutnya dari algoritma RC4 dinamakan Pseudo-random Generation Algorithm (PRGA). Tahap ini menghasilkan nilai pseudo-random yang kemudian dilakukan operasi XOR dengan plaintext untuk proses enkripsi atau dengan ciphertext pada proses dekripsi. Untuk langkah-langkah PRGA adalah sebagai berikut [8]:

1. Inisialisasikan nilai *i =* 0 dan *j* = 0
2. Hitung nilai *i* dan *j* yang baru.
3. Lakukan Swaping pada nilai *S*[*i*] dengan *S*[*j*].
4. Hitung nilai .
5. Ambil nilai S[t] kemudian lakukan operasi XOR pada plaintext ataupun ciphertext dengan indeks k.
6. Lakukan langkah kedua hingga kelima untuk setiap nilai k = 0, k = 1, …, k = n – 1.

Contoh pada *key schedulling* menghasilkan larik S seperti yang ditunjukkan oleh tabel 2.4 dan pesan yang akan dienkripsi adalah “jaya” dengan kode ASCII 106, 97, 121 dan 97. Ciphertext akan dihitung dengan menginisialisasikan nilai i dan j dengan nol. Selanjutnya, dari nilai nol sampai dengan panjang dari pesan dikurangi satu yaitu bernilai tiga, dilakukan perhitungan nilai i dan j yang baru. Hasil perhitungan pertama adalah:

Nilai S[1] = 103 dan S[103] = 30 ditukarkan sehingga dihasilkan S[1] = 30 dan S[103] = 103. Selanjutnya akan dilakukan perhitungan nilai t. Hasil perhitungan nilai t adalah:

Sehingga didapat nilai *S*[*t*] = *S*[133] dimana *S*[133] = 120. Kemudian nilai *S*[133] akan di-*XOR*kan dengan pesan[*k*] = pesan[0] dimana pesan[0] yaitu “j” dengan kode ASCII sama dengan 106. Hasil perhitungannya adalah:

|  |  |  |
| --- | --- | --- |
| 120 | 0111 | 1000 |
| 106 | 0110 | 1010 |
|  | 0001 | 0010 |

# 3. METODOLOGI PENELITIAN

**Bahan penelitian**

Bahan penelitian ini adalah sebuah teks sebagai plainteks dan diproses menjadi chiperteks melalui enkripsi.

Penelitian ini akan membuat antarmuka aplikasi kriptografi teks. Kemudian dalam penlitian ini juga akan menginplementasikan algoritma *vigenere chiper* dan RC4 ke dalam sebuah aplikasi berbasis web. Hasil dari proses enkripsi tersebut juga berupa teks, namun telah terenkripsi. Teks yang telah terenkripsi tersebut akan didekripsi untuk mengembalikan menjadi plainteks atau teks asli agar pesan dapat dibaca. Alur penelitian dalam sistem keamanan teks tersebut dapat Gambar 3.1



Gambar 3.1 Jalan Penelitian.

**Data Flow Diagram (DFD)**

Data Flow Diagram (DFD) merupakan diagram alir data yang menggambarkan bagaimana data diproses oleh sistem.

1. Diagram konteks memiliki sebuah proses yaitu untuk penentuan penyakit lambung pada manusia dengan tiga entity yaitu pasien, admin dan user seperti pada Gambar 3.2.



Gambar 3.2 Diagram Konteks.

1. DFD level 0 yang merupakan penjabaran dari diagram konteks, dapat dilihat pada Gambar 3.3.



Gambar 3.3 DFD level 0

1. DFD Level 1 proses pengenkripsi dan pendekripsian dari 2 metode yaitu metode vigenre dan RC4 dapat dilihat pada Gambar 3.4 dan 3.5.



Gambar 3.4 Proses Enkripsi.



Gambar 4.5 Proses Dekripsi.

# 4. PEMBAHASAN

Analisa dalam penelitian ini bertujuan untuk mengetahui bagaimana unjuk kerja aplikasi ini, yaitu mengubah plaintext menjadi ciphertext. Untuk mengetahui unjuk kerja algoritma dalam mengenkripsi dan mendekripsi teks sesuai pesan aslinya, dilakukan uji coba secara berulang-ulang.

Aplikasi ini mengenkripsi pesan sebanyak dua kali secara berurutan, yaitu algoritma vigerene cipher terlebih dahulu kemudia ciphertext dienkripsi kembali dengan algoritma RC4. Contoh enkripsi dapat dilihat pada Gambar 4.1.



Gambar 4. 1 Proses Enkripsi.

Proses dekripsi merupakan proses kebalikan dari enkripsi teks yang telah dienkripsi akan diubah kembali menjadi teks asli. Seperti pada proses enkripsi, proses dekripsi juga menggunakan dua algoritma yang dijalankan secara berurutan. Namun urutannya menjadi RC4 yang dijalan terlebih dahulu, kemudian dilanjutkan algoritma vigenere cipher dengan memasukan kunci yang sama pada saat enkripsi. Maka akan didapatkan teks aslinya. Tampilan dekripsinya dapat dilihat pada Gambar 4.2.



Gambar 4.2 Proses Dekripsi.

Pengujian ini bertujuan untuk mengetahui bagaimana kinerja sistem dalam aplikasi ini. Pengujian ini akan menjawab apakah aplikasi ini dapat berfungsi dengan baik sesuai dengan tujuan penelitian atau ada kekurangan dalam sistem.

Halaman hanya menampilan satu menu yang digunakan pengguna untuk menuju ke halaman proses enkripsi dan dekripsi. Tampilan halaman pertama dapat dilihat pada Gambar 4.3.



Gambar 4.3 Tampilan Aplikasi.

Pengujian dilakukan dengan dua cara. Pertama, pengujian enkripsi dengan kunci yang benar. Kedua, pengujian dekripsi dengan kunci yang salah. Kedua pengujian tersebut menggunakan pesan yang sama, namun pada pengujian kedua kunci dekripsi menggunakan kunci yang berbeda. Jenis pesan yang digunakan adalah kata dan simbol, kalimat, halaman, paragraf dan dokumen. Hasil pengujian dapat dilihat pada Tabel 4.1.

Tabel 4. 1 Tabel Pengujian.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No | Plainteks | KunciVigenere | Cipherteks | KunciRC4 | CipherteksRC4 | Ket |
| B | TB |
| 1 | Berangkat | Oke | povoxkykx | Siap | F2AB5F45F5CB97CFA2 | B | - |
| 2 | Makan | Siap | Eikpf | Buah | 06E5B7BC05 | B | - |
| 3 | Angka | Dua | Dhgnu | Halo | 3A5FBAB332 | B | - |
| 4 | Ngantuk | Zzz | Mfzmstj | Slep | 5807F8A96BF33B | B | - |
| 5 | Masuk | In | Unahs | Out | C558C3BBFC | B | - |
| 6 | Diskon 100% | Toko | wwcyhb 100% | Baju | 167F49B3E6AC973EEB3284 | B | - |

# 5. PENUTUP

**Kesimpulan**

Kesimpulan yang didapat dari hasil penelitian teknik kriptografi pengenkripsian sebuah teks dengan metode vigenere cipher dan RC4, maka dapat disimpulkan bahwa:

1. Aplikasi yang dirancang dalam penelitian ini mampu melakukan enkripsi dan dekripsi.
2. Dari 30 data yang diujikan tingkat keberhasilnya mencapai 100%.
3. Hasil mengujian enkripsi dan dekripsi mampu memuat seperti simbol khusus, angka dan gabungan kata dan simbol.

**Saran**

Berdasarkan pengujian terhadap teknik teknik kriptografi pengenkripsian sebuah teks dengan metode vigenere cipher dan RC4, saran yang dapat diberikan sehubungan dengan penelitian tersebut adalah sebagai berikut:

1. Pada aplikasi ini hanya data mengenkripsi dan mendekripsi data yang berupa teks, diharapkan pada penelitian selanjut data dapat berupa teks dan yang lainnya.
2. Aplikasi pada penelitian ini hanya diterapkan pada aplikasi berbasis web, diharapkan pada penelitian selanjutnya dapat diterapkan diplatform yang lain seperti android.

# 6. UCAPAN TERIMA KASIH

Penulis ingin mengucapkan terimakasih kepada seluruh pihak yang ikut terlibat diantaranya dosen pembimbing Universitas Mercu Buana Yogyakarta dan Teman-Teman sekalian.

# DAFTAR PUSTAKA

Amirudin, R. (2016). Implementasi Algoritma Kriptografi RC4 dan Vigenere Chiper Pada Citra Bitmap.

Efrandi, Asnawati, & Yupiyanti. (2014). Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher. *Jurnal Media Infotama*, 120-128, ISSN 1858 – 2680, Vol.2.

Hakin, E. L., Khairil, & Utami, F. H. (2014). Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma Rc4 Dengan Menggunakan Bahasa Pemrograman Php. *Jurnal Media Infotama*, 1-6;ISSN 1858 – 2680.

Irawan, M. D. (2017). Implementasi Kriptografi Vigenere Cipher Dengan Php. *Jurnla Teknologi Informasi*, 11-21, ISSN : 2580-7927.

kormodimoeljo, s. (2009). *Teori dan Aplikasi Kriptografi.* SPK IT Consulting.

Kurniawan, S. T., Dedih, & Supriyadi. (2017). mplementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks Berbasis Android. *Jurnal Online Informatika*, 102-109, ISSN : 2527-1682, Vol.2 No.2.

Maricar, M. A., & Sastra, N. P. (2018). Efektivitas Pesan Teks dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi. *Majalah Ilmiah Teknologi Elektro*, Hal 59-64 : Vol.17.

Mukhtar, H. (2018). *Kriptografi Untuk Keamanan Data.* Ngaglik, Sleman: Grub Penerbitan CV Budi Utama.

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Jurnal Infromatika Mulawarman*, 20-31.

Putra, M. D., & Hayati, M. (2018). Enkripsi Dan Dekripsi Gambar Dengan Menggunakan Perpaduan Algoritma Base64 Dan Rc4. *Seminar Nasional Teknologi Informasi dan Multimedia*, 2.14-1 - 2.14-6; ISSN:2302-3805.

Rahmawati, D., & Candra, A. (2015). Implementasi Kombinasi Caesar dan Affine. *Jurnal Edukasi dan Penelitian Informatika (JEPIN) Vol. 1, No. 2*, 60-63.

Simamora, D. P O. (2017). Implementasi Algoritma RC4 dan Playfair Cipher Untuk Mengamankan Data Teks. *Jurnal Pelita Informatika*, 328-334 ; ISSN : 2301-9425.

Sinaga, D., & Umam, C. (2018). Implementasi Kriptografi Vigenere Cipher Pada Media Teks Dengan Kombinasi Transposisi Kolom. 136-139; ISSN:978-979-3649-99-3.

Sobur, A. (2004). *Semiotika Komunikasi.* Bandung: Remaja Rosdakarya.

Tanjung, P. S. (2017). Implementasi Pengamanan Data Teks Dengan Metode International Data Encryption Algorithm (Idea) Dan Rivest Code (Rc4) Berbasis Android.