Volume 4 Nomor 2 Mei 2019

INFORMASI INTERAKTIF

JURNAL INFORMATIKA DAN TEKNOLOGI INFORMASI

PROGRAM STUDI TEKNIK INFORMATIKA – FAKULTAS TEKNIK -UNIVERSITAS JANABADRA

INFORMASI INTERAKTIF	Vol. 4	No. 2	Hal. 63 - 130	Yogyakarta Mei 2019	ISSN 2527-5240

ISSN 2527-5240

DEWAN EDITORIAL

JURNAL INFORMASI INTERAKTIF merupakan media komunikasi hasil penelitian, studi kasus, dan ulasan ilmiah bagi ilmuwan dan praktisi dibidang Teknik Iinformatika. Diterbitkan oleh Program Studi Teknik Informatika Fakultas Teknik Universitas Janabadra di Yogyakarta, tiga kali setahun pada bulan Januari, Mei dan September.

ISSN 2527-5240

DAFTAR ISI

ISSN 2527-5240

PENGANTAR REDAKSI

Puji syukur kami panjatkan kehadirat Allah Tuhan Yang Maha Kuasa atas terbitnya JURNAL INFORMASI INTERAKTIF Volume 4, Nomor 2, Edisi Mei 2019. Pada edisi kali ini memuat 9 (sembilan) tulisan hasil penelitian dalam bidang teknik informatika.

Harapan kami semoga naskah yang tersaji dalam JURNAL INFORMASI INTERAKTIF edisi Januari tahun 2019 dapat menambah pengetahuan dan wawasan di bidangnya masing-masing dan bagi penulis, jurnal ini diharapkan menjadi salah satu wadah untuk berbagi hasil-hasil penelitian yang telah dilakukan kepada seluruh akademisi maupun masyarakat pada umumnya.

Redaksi

MODIFIKASI KRIPTOGRAFI KLASIK *VIGENERE CIPHER* MENGGUNAKAN *ONE TIME PAD* DENGAN ENKRIPSI BERLANJUT

M. Ziaurrahman[1], Ema Utami[2], Ferry Wahyu Wibowo[3]

[1,2,3] Magister Teknik Informatika, Universitas AMIKOM Yogyakarta
Jl. Ringroad Utara, Condongcatur, Depok, Sleman, Yogyakarta Indonesia 55283

E-Mail : [1]m.ziaurrahman1994@gmail.com, [2]ema.u@amikom.ac.id, [3]ferry.w@amikom.ac.id

ABSTRACT

The development of communication is increasingly rapid which does not escape from various threats such as eavesdropping or data theft, because that security aspect of data security is now very calculated. Various ways have been done to secure data that contains confidential information. One method used is to scramble the data into unclear content, so that when tapped it will be difficult to find out the actual information content. Encryption techniques by changing and randomizing the original form of data are called cryptography. Vigenere cipher is one type of classical cryptography algorithm that is popular and often used. This Vigenere cipher uses a substitution technique in encrypting the message where each plaintext character in the message will be encrypted into another character in the ciphertext based on the key used. One Pad algorithm is one algorithm that has perfection when encrypting and decrypting it. The basic concept of the One Time Pad algorithm is almost the same as the Vigenere algorithm, except that in this algorithm the key is generated randomly. In this paper, we will explain how to strengthen Vigenere cipher by modifying Vigenere ciphers. Modifications are carried out by applying One Time Pad encryption generated from the key and the next key generation technique using Vigenere encryption continues so that the key used for the coding will be different from the key used previously. With the use of this method, the connection between plaintext and ciphertext will become less and more difficult to solve cryptanalis.

Keywords: *Cryptography, Modification, Vigenere Cipher, One Time Pad, and Cyber Security*.

1. PENDAHULUAN

Di zaman ini teknologi sudah semakin canggih, hampir semua kalangan sudah menggunakan teknologi baik itu masyarakat, pejabat pemerintah atau orang penting lainnya. Banyak di antara mereka me-manfaatkan teknologi untuk bertukar infor-masi di antaranya yang bersifat pribadi atau rahasia. Keamanan dari informasi tersebut merupakan hal yang sangat penting untuk dijaga, terutama jika itu berkaitan dengan masalah keamanan suatu negara, kebijakan-kebijakan bisnis suatu perusahaan dan informasi-informasi penting lainnya yang akan berakibat fatal jika disalah-gunakan oleh pihak yang tidak bertanggung jawab. Berdasarkan hasil survey yang dilakukan oleh *High Technology Crime Investigation Associations* (HTCIA) dari 445 responden, sekitar 14% membutuhkan peningkatan keamanan pada data, yaitu peningkatan privacy dan policy yang lebih baik dan 56,4% membutuhkan pelatihan dan pengetahuan tentang pengamanan data pada komputer atau jaringan [1].

Bagi beberapa individu, kelompok, kantor, lembaga, dan negara informasi merupakan suatu hal yang sangat penting. Dilihat dari sifatnya informasi dapat bersifat rahasia atau tidak rahasia, mereka yang menganggap informasi tersebut penting dan rahasia pasti akan berusaha untuk melin-dungi kerahasiaan dari informasi yang di simpan atau di komunikasikan tersebut. Hal ini menunjukan keamanan komputer sangat dibutuhkan untuk mencegah timbulnya lebih banyak kerugian. Tujuan utama keamanan komputer yaitu menjaga kerahasiaan data (*confidentiality*), menjaga agar data tetap utuh (*integrity*), dan menyediakan data ketika diperlukan (*availability*) [2].

Berbagai macam cara telah dilakukan untuk mengamankan data yang berisi informasi rahasia ini. Salah satu cara yang digunakan adalah dengan cara mengacak data sehingga menjadi tidak jelas isinya, sehingga apabila disadap maka orang yang tidak bertanggung jawab akan kesulitan untuk mengetahui isi informasi yang sebenarnya. Teknik penyandian dengan mengubah dan mengacak bentuk asli dari data disebut dengan

kriptografi. Dengan menggunakan teknik enkripsi terhadap integritas data maka suatu informasi tidak bisa dibaca oleh orang yang tidak berkepentingan [3].

2. LANDASAN TEORI

2.1 Sejarah Kriptografi

Kriptografi telah digunakan oleh bangsa Mesir sejak sekitar 4000 tahun yang lalu, dimasa itu tulisan yang digunakan bangsa Mesir masih berupa hieroglyph tidak standard yang digunakan untuk menulis pesan pada piramid. Sedangkan bangsa Yunani telah menggunakan kriptografi sejak sekitar 400 tahun yang lalu sebelum masehi, disaat itu bangsa Yunani menggunakan alat yang bernama *scytale* untuk menyampaikan pesan. *Scytale* adalah kertas panjang yang digulung pada sebuah kayu, pesan ditulis secara horizontal secara baris per baris, apabila kertas dilepaskan, maka pesan akan berubah menjadi huruf-huruf sandi yang sulit untuk diterjemahkan. Dengan cara ini lah bangsa Yunani menyampaikan pesan rahasia kepada pihak-pihak yang bersangkutan [7].

Peradaban Islam juga menemukan kriptografi karena penguasaannya terhadap matematika, statistik, dan linguistik. Bahkan teknik kriptanalisis dipaparkan untuk pertama kalinya pada abad 9 M oleh seorang ilmuwan bernama Abu Yusuf Ya'qub ibn 'Ishaq as-Shabbah al Kindi atau dikenal dengan Al-Kindi yang menulis kitab tentang seni memecahkan kode. Kitabnya berjudul Risalah fi Istikhraj al-Mu'amma (Manuskrip untuk memecahkan pesan-pesan Kriptografi). Terinspirasi dari perulangan huruf dalam Al-Qur'an, Al-Kindi menemukan teknik analisis frekuensi, yakni teknik untuk memecahkan ciphertext berdasarkan frekuensi kemunculan karakter pada sebuah pesan [8].

Setelah abad ke-20, karena pesatnya teknologi informmasi membuat kriptografi bukan lagi hanya sebatas ilmu, kriptografi mulai di teliti dan mulai digunakan untuk keamanan data. Kriptografi sering dipakai pada bidang kemiliteran, contoh dari penerapan yang nyata, kriptografi dipakai dalam Perang Dunia II oleh Pemerintahan Nazi Jerman yang menggunakan mesin Enigma dalam mengubah pesan standart menjadi pesan rahasia [7].

2.2 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *kryptos* yang berarti tersembunyi dan *graphein* yang bermakna tulisan. Kriptografi adalah ilmu menulis pesan rahasia yang mana bertujuan untuk menyembunyikan makna sesungguhnya dari pesan tersebut. Tetapi seiring perkembangan zaman hingga saat ini pengertian kriptografi berkembang menjadi ilmu tentang teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa privasi dan otentikasi [3][9].

Dalam kriptografi sendiri terdapat beberapa istilah, yaitu [4] :

1. *Plaintext* merupakan pesan asli sebelum diubah menjadi pesan rahasia.
2. *Key* merupakan kunci rahasia yang digunakan untuk mengubah atau mengembalikan pesan rahasia.
3. *Ciphertext* merupakan pesan rahasia yang telah diubah bentuknya menjadi kode-kode yang sukar diterjemahkan.
4. Enkripsi merupakan proses pengubahan plaintext menjadi ciphertext.
5. Dekripsi merupakan proses pengembalian ciphertext menjadi plaintext.

2.3 Jenis Kriptografi

Berdasarkan perkembangan dari tahun ke tahun sejak pertama kali kriptografi ditemukan, ada dua jenis algoritma kriptografi, yaitu :

1. Kriptografi Klasik

   Algoritma kriptografi yang termasuk kedalam kriptografi klasik ini digunakan sejak sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Metode menyembunyikan pesannya adalah dengan teknik substitusi atau transposisi atau keduanya [5]. Teknik substitusi bekrja dengan cara menggantikan karakter dalam plaintext menjadi karakter lain yang hasil akhirnya adalah *ciphertext*. Sedangkan transposisi merupakan teknik untuk mengubah *plaintext* menjadi *ciphertext* dengan cara permutasi karakter. Kombinasi dari keduanya sebenarnya yang secara kompleks yang melatar belakangi terbentuknya berbagai macam algoritma kriptografi modern [6].

2. Kriptografi Modern

   Algoritma kriptografi yang termasuk ke dalam jenis kriptografi modern dengan memiliki tingkat kesulitan yang kompleks, dan kekuatan kriptografinya ada pada key atau kuncinya. Kriptografi modern menggunakan pengolahan simbol biner karena berjalan mengikuti operasi komputer digital, sehingga membutuhkan dasar berupa pengetahuan terhadap matematika untuk bias mempelajari dan menguasainya [5][6].

2.4 Vigenere Cipher

Algoritma Vigenere Cipher adalah bagian dari kriptografi polialfabetik yang ditemukan pertama kali pada tahun 1586 oleh diplomat Perancis yang bernama Blaise de Vigenere (1523-1596). Vigenere cipher merupakan jenis cipher abjad majemuk yang paling sederhana. Vigenere cipher menerapkan metode substitusi poli alfabetik dan termasuk ke dalam kategori kunci simetris dimana kunci yang digunakan untuk proses enkripsi adalah sama dengan kunci yang digunakan untuk proses dekripsi.Tujuan utama dari Vigenere cipher ini adalah menyembunyikan keterhubungan antara plainteks dan cipherteks dengan menggunakan kata kunci sebagai penentu pergeseran karakternya [13].

Viginere cipher menggunakan tabel vigenere standart dalam mengenkripsi pesan. Tabel yang digunakan merupakan tabel 26 huruf alfabetik standart, yang dimulai dari A sampai Z. Kunci pada Vigenere Cipher dipakai berulang kali sebanyak pesan yang akan dienkripsi. Semakin beragam huruf alfabetik yang dipakai sebagai kunci, maka semakin kuat juga keamanan algoritma Vigenere Cipher ini. Berikut ini rumus enkripsi dan dekripsi Vigenere Cipher :

Enkripsi : Ci = Pi + ki mod 26…….. (1)
Dekripsi : Pi = Ci - ki mod 26…… (2)

2.5 *One Time Pad*

One Time Pad juga biasa dikenal sebagai versi perbaikan dari algoritma *Vernam Cipher* untuk menghasilkan keamanan yang sempurna, pertamakali ditemukan oleh Gillbert Vernam pada tahun 1917 di Major Joseph Mauborge and AT & T's. Konsep dasar dari algoritma *One Time Pad* sendiri hampir sama dengan pendahulunya algoritma *Vigenere. One-time pad* (OTP) adalah stream cipher yang melakukan enkripsi dan dekripsi satu karakter berkali-kali [11].

Untuk melakukan enkripsi karakter alpabet dapat dinyatakan sebagai penjumlahan modulo 26 dari satu karakter plainteks dengan satu karakter kunci *one-time pad*:

Ci = Pi + ki mod 26 …….....(3)

Jika karakter yang digunakan adalah anggota himpunan 256 karakter (seperti karakter dengan pengkodean ASCII), maka persamaan enkripsinya menjadi [12]:

Dekripsi : Pi = Ci - ki mod 26…….(4)

Setelah pengirim mengenkripsi pesan dengan kunci, ia menghancurkan kunci tersebut. Penerima pesan menggunakan pad yang sama untuk mendekripsikan karakter-karakter cipherteks menjadi karakter-karakter plainteks dengan persamaan [12]:

p i = (c i – k i) mod 26……(5)

untuk alfabet 26-huruf, atau

p i = (c i – k i) mod 256 …….(6)

untuk alfabet 256-karakter.

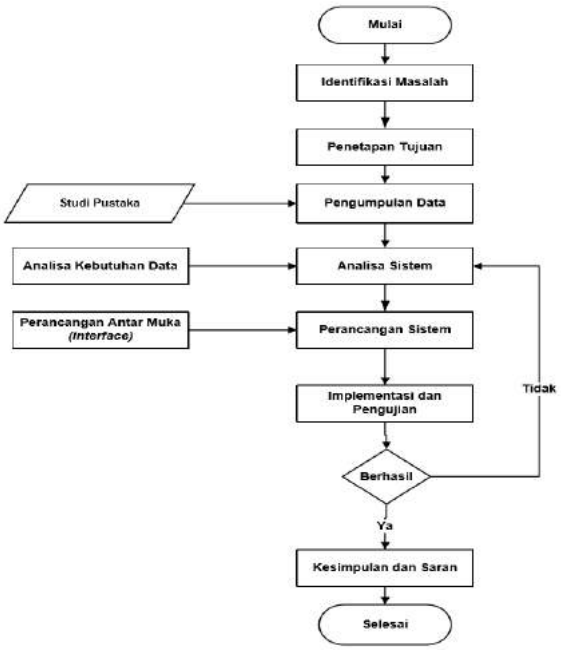
Perhatikan bahwa panjang kunci harus sama dengan panjang plainteks, sehingga tidak ada kebutuhan mengulang penggunaan kunci selama proses enkripsi (seperti halnya pada Vernam cipher) [11].

Algoritma OTP ini tidak dapat dipecahkan (unbreakable) karena dua alasan:

1. Barisan kunci acak yang ditambahkan ke pesan plainteks yang tidak acak menghasilkan cipherteks yang seluruhnya acak. Cipherteks ini tidak mempunyai hubungan statistik dengan plainteks [10].
2. Karena cipherteks tidak mengandung informasi apapun perihal plainteks, maka tidak mungkin ada cara untuk memecahkan cipherteks. Beberapa barisan kunci yang digunakan untuk mendekripsi cipherteks mungkin menghasilkan plainteks yang mempunyai makna, sehingga kriptanalis tidak punya cara untuk menentukan plainteks mana yang benar.

3. METODE PENELITIAN

Diagram alir sangat berguna bagi semua orang yang membuat perancangan yang akan dibuat. Dimana diagram selalu berisi tentang algoritma yang dipakai, proses dan langkah-langkah yang disimbolkan kedalam bentuk kotak dan urutanya dengan cara saling menghubungkan langkah-langkah satu sama lain dengan menggunakan simbol panah Seperti pada gambar 1 dibawah ini.



Gambar 1 Alur penelitian

Diagram alir data menggambarkan alur penelitian dalam melakukan modifikasi teknik kriptografi klasik viginere cipher.

Dalam penelitian yang dilakukan terdapat beberapa metode yang mencakup beberapa bagian yaitu sebagai berikut: Penelitian ini adalah penelitian yang berjenis eksperimental. Penelitian eksperi-mental adalah penelitian dengan mencatat langsung hasil pengujian atau percobaanya dalam pengum-pulan data.

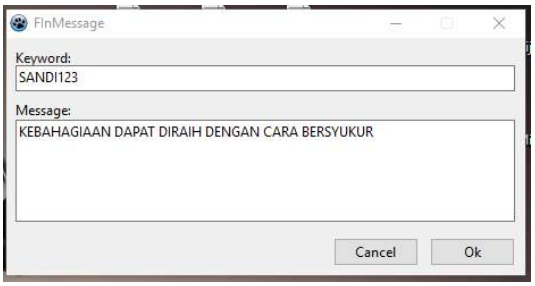
Di dalam sebuah penelitian diperlukan sebuah data yang nantinya diperlukan dalam penelitian, berikut beberapa metode pengumpulan data yang akan digunakan :

a. Metode studi literatur merupakan metode pengumpulan data dengan cara mencari dari berbagai sumber tertulis seperti buku-buku, jurnal, internet dan pustaka. Metode ini dilakukan untuk mengumpulkan data-data yang berkaitan dengan penelitian yang dijalani. Data-data yang dikumpulkan dari hasil studi pustaka ini adalah Spesifikasi perangkat keras dan perangkat lunak yang digunakan, Data yang berkaitan dengan kriptografi dan dari dua metode yang di gunakan yaitu metode *vigenere cipher* dan metode *one time pad* mengenai cara atau langkah-langkah dalam penerapannya.

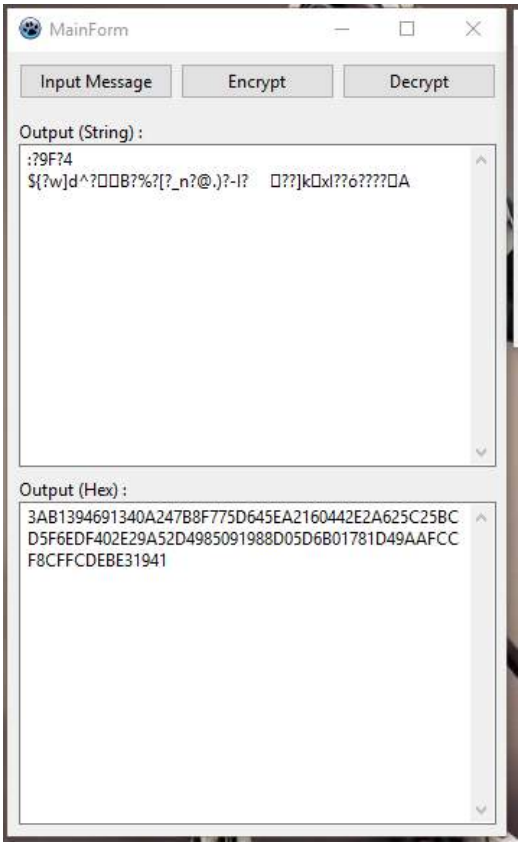
b. Metode eksperimen merupakan pengumpulan data menggunakan suatu cara dengan mengadakan beberapa percobaan terhadap sesuatu hal yang berbeda berkaitan dengan penelitian yang diteliti. Di metode ini akan dikumpulkan data-data yaitu mengenai pembuatan program, dan perbedaan antara kedua metode dari hasil program yang telah dibuat nantinya.

4. HASIL DAN PEMBAHASAN

Dibawah ini adalah gambar jendela input key dan pesan yang akan di enkripsi.



Gambar 2 Tampilan input key dan pesan



Gambar 3 Tampilan utama aplikasi

Penelitian ini menghasilkan sebuah metode modifikasi kriptograpi yang bisa digunakan untuk mengamankan data dengan memodifikasi metode vigenere cipher me-nggunakan one time pad.

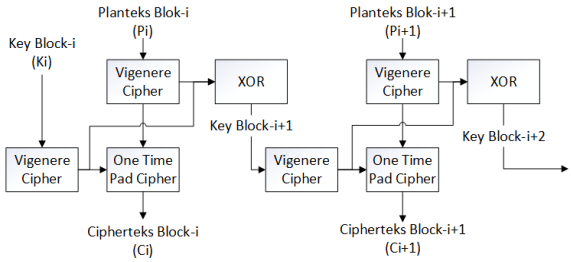
Vigenere cipher bukanlah algoritma kriptografi yang unbreakable, terutama dari serangan kriptanalist. Namun, bukan berarti tidak ada hal yang bisa dilakukan untuk memperkuat Vigenerer Cipher dari serangan kriptanalis. Dapat dilakukan teknik-teknik modifikasi tertentu untuk menyamarkan keter-hubungan antara plainteks dan cipher-teksnya.

Modifikasi yang dilakukan harus dapat mengurangi kemunculan key yang berulang atau bahkan menggunakan pendekatan One-Pad kriptografi yang mana panjang key adalah sama dengan panjang plainteks yang digunakan dimana key akan digenerate berbeda dengan key yang digunakan sebelumnya.

Modifikasi Viginere Cipher yang dilakukan disini adalah bukan modifikasi pada algoritma utamanya.

Bentuk modifikasi yang dilakukan untuk proses ENKRIPSI adalah :

1. Plaintext dan Key yang di inputkan terlebih dahulu di ubah kedalam bentuk hex.
2. Plaintext dibagi menjadi blok-blok yang mana didasarkan dari panjangnya key yang digunakan.
3. Pada pemrosesan key blok-i akan menggunakan key yang di inputkan dan kemudian di enkripsi dengan vegenere cipher, key Ki lainnya masing-masing di bangkitkan berdasarkan blok-i sebelumnya dan di XOR kan dengan hasil vigenere cipher di blok sebelumnya hingga keseluruhan plaintext habis.
4. Di tiap-tiap blok plaintext-i (Pi) akan di enkripsi terlebih dahulu dengan vigenere cipher. Pengambilan dari vigenere cipher didasarkan pada pengambilan tiap-tiap bit pada plaintext.
5. Hasil enkripsi Pi tadi kemudian di enkripsi lagi menggunakan one time pad yang nantinya akan membentuk cipher block-i (Ci), key pembanding yang digunakan adalah Ki yang telah di enkripsi dengan vigenere cipher sebelumnya.



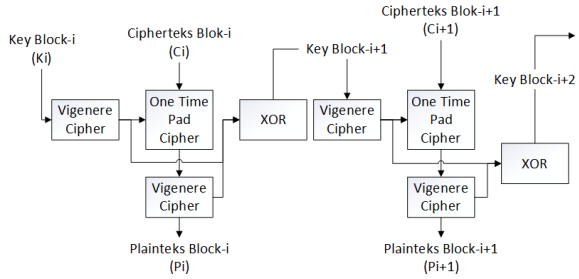
Gambar 4 Skema Enkripsi Vigenere Modifikasi

Bentuk modifikasi yang dilakukan untuk proses DEKRIPSI adalah :

1. Ciphertext dan Key yang di inputkan dan belum di konversi kedalam bentuk hex harus di rubah ke bentuk hex.
2. Ciphertext dibagi menjadi blok-blok yang mana didasarkan dari panjangnya key yang digunakan.
3. Pada pemrosesan key blok-i akan menggunakan key yang di inputkan dan di enkripsi dengan vigenere cipher kemudian hasil enkripsi tadi digunakan sebagai key untuk mendekrip ciphertext dengan one time pad, key Ki lainnya masing-masing di bangkitkan

berdasarkan blok-i sebelumnya dan di XOR kan dengan hasil vigenere cipher di blok sebelumnya hingga keseluruhan ciphertext habis.

4. Hasil dekripsi Ci tadi kemudian di dekripsi lagi menggunakan vigenere cipher yang nantinya akan membentuk plaintext block-i (Pi), key pembanding yang digunakan adalah Ki yang telah di enkripsi dengan vigenere cipher sebelumnya.



Gambar 5 Skema Dekripsi Vigenere Modifikasi

Blok plainteks yang dibentuk didasarkan pada Panjang dari key yang di masukan. Pengenkripsian dan pendekripsian dilakukan bertahap dengan perblok.

Fungsi pembangkitan key baru dengan metode vigenere cipher pada bentuk modifikasi ini adalah untuk meningkatkan keamanan dan mengurangi keterkaitan berulang yang menjadi kelemahan vigenere cipher serta keterhubungan antara teks sebelum enkripsi dan teks sesudah enkripsi.

Fungsi dari penggunaan One Time Pad adalah sebagai lapisan tambahan dalam pengacakan data sehingga tatanan dan susunan karakter menjadi rusak, sebagai bentuk pencegahan terhadap kriptanalis sehingga metode analisis frekuensi tidak dapat dijadikan sebagai acuan untuk memecahkan kode hasil enkripsi.

5. KESIMPULAN

Dari analisis, perancangan, dan pengujian modifikasi algoritma kriptografi *Vigenere cipher* menggunakan *One Time Pad*, didapat kesimpulan sebagai berikut :

1. Algoritma vigenere cipher merupakan satu dari sekian banyak algoritma kriptografi klasik yang cukup popular, mudah, dan sederhana penggunaannya.
2. Vigenere cipher dari hasil modifikasi lebih aman dan lebih sulit diserang oleh kriptanalis dibandingkan vigenere cipher biasa.
3. Modifikasi algoritma vigenere cipher modifikasi ini telah dapat menghilangkan kekurangan yang mana kadang keter-hubungan karakter dari plainteks dan cipherteks sehingga tak mudah di identifikasi dan cukup sulit dipecahkan.
4. Penggunaan vigenere cipher modifikasi dengan key yang panjang dan bervariasi akan meningkatkan tingkat keamanan, hal ini terjadi karena blok yang digunakan menggunakan panjang dari kunci.

DAFTAR PUSTAKA

[1] Monkhouse, H. Duncan. (2011). Repost on Cyber Crime Investigation. HTCIA.Inc.

[2] Simarmata, Janner. 2006. Pengenalan Teknologi dan Informasi. Yogyakarta: Andi.

[3] Atika Sari, Christy., Hari Rachmawanto, Eko. 2014. Gabungan Algoritma Vernam Cipher dan End Of File untuk Keamanan Data. Jurnal. Techno.Com, Vol.13, No.3, Agustus 2014 : 150-157.

[4] Paar, Christof., Pelzi, Jan., dan Preneel, Bart.2010. Understanding Cryptography. Springer.

[5] Sadikin, Rifki. 2012. Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java. Penerbit Andi, Yogyakarta.

[6] Prayudi, Yudi, Idham Halik. 2005. Studi Analisis Algoritma Rivest Code 6 (RC6) Dalam Enkripsi/Dekripsi Data. Seminar Nasional Aplikasi Teknologi Informasi 2005 (SNATI 2005), Yogyakarta.

[7] Kahn, D. (1996). The Codebreakers: The comprehensive history of secret communication from ancient times to the internet. Simon and Schuster.

[8] Wirdasari, Dian. 2008. Prinsip Kerja Kriptografi dalam Mengamankan Informasi, Jurnal SAINTIKOM Vol.5 No.2.

[9] Diffie, Whitfield, Martin E Hellman. 1976. New Directions in Cryptography. IEEE Trans. Info. Theory IT-22.

[10] William Stalling, 2003, Cryptography and Network Security, Principle and Practice 3 rd Edition, Pearson Education, Inc.

[11] Deng, F. G., & Long, G. L. (2004). Secure direct communication with a quantum one-time pad. Physical Review A, 69(5), 052319.

[12] Rubin, F. (1996). One-time pad cryptography. Cryptologia, 20(4), 359-364.

[13] Andhika, Fatardhi Rizky. 2011. Modifikasi Vigenere Cipher dengan Menggunakan Caesar Cipher dan Enkripsi Berlanjut untuk Pembentukan Key-nya. Bandung. ITB,