Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 1, September 2020
e-ISSN 2685-998X
DOI 10.30865/json.v2i1.2457

Penerapan Algoritma *Venigmare Cipher* dan *Vernam Cipher* Dalam Pengamanan Data Teks

Kermanosiavic Noverdianto Siahaan, Mesran

Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: Kermanosiavic@gmail.com, mesran.skom.mkom@gmail.com
Submitted: **02/09/2020**; Accepted: **27/09/2020**; Published: **30/09/2020**

Abstrak–Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam sistem informasi pada saat ini. Munculnya teknologi internet dan multimedia telah mendorong berbagai macam usaha untuk melindungi, mengamankan, dan menyembunyikan data pada file digital dari pihak-pihak yang tidak mempunyai otoritas untuk mengakses file-file tersebut. Salah satu usaha untuk mengamankan data dan informasi diantaranya dengan menggunakan venigmare cihper dan vernam cihper. Venigmare adalah enkripsi yang mampu mengurangi korelasi antara frekuensi huruf pada plaintext dan Ciphertext. Tetapi sayangnya metode ini masih menyisakan pola yang berulang, apalagi jika plaintext yang di enkripsi cukup panjang, Dalam hal ini, peran teknik penyandian data yang dikenal dengan nama kriptografi sangat penting. Kriptografi merupakanteknik untuk menyandikan data melalui proses ekripsi dan dekripsi dengan kunci tertentu sehingga menghasilkan data tersandikan yang tidak diketahui oleh orang lain. Dalam makalah ini akan digunakan algoritma vernam cipher

Kata Kunci: Kriptografi, Keamanan, File Teks, Venigmare Chiper, Vernam Chiper

Abstract–Data security and confidentiality is one very important aspect in today's information system. The emergence of internet and multimedia technology has prompted various efforts to protect, secure, and hide data on digital files from unauthorized parties to access these files. One of the efforts to secure data and information includes using the Venigmare Cihper and the Vernam Cihper. Venigmare is an encryption that can reduce the correlation between the frequency of letters in plaintext and Ciphertext. But unfortunately this method still leaves a repeating pattern, especially if the encrypted plaintext is long enough. In this case, the role of the data encryption technique known as cryptography is very important. Cryptography is a technique for encoding data through a process of encryption and decryption with a specific key to produce encrypted data that is unknown to others. This paper will use the Vernam Cipher algorithm.

Keywords: Cryptography, Security, Text Files, Venigmare Chiper, Vernam Chiper.

1. PENDAHULUAN

Masalah keamanan merupakan salah satu aspek paling penting dalam dunia teknologi informasi, misalnya : keamanan file teks. Sekarang ini, sebagian besar dokumen-dokumen menggunakan aplikasi pengolahan teks, karena kemudahan dalam menggunakannya. Berbagai aplikasi didalam komputer dapat digunakan untuk mengolah kata dan angka sesuai kebutuhan pengguna. Keamanan file (dokumen) sangat diperlukan, maka setiap orang memerlukan suatu aplikasi yang dapat mengamankan dokumen rahasia dan penting agar dokumen tersebut hanya dapat di lihat dan di baca oleh orang tertentu saja. Beberapa cara telah dikembangkan untuk menangani masalah keamanan ini, salah satu teknik untuk pengamanan data adalah dengan menggunakan algoritma penyandian data. Algoritma penyandian data saat ini telah semakin banyak jumlahnya, sejalan dengan berkembangnya ilmu yang mempelajari penyandian data tersebut. Ilmu ini biasa disebut Kriptografi.

Dalam menjaga keamanan data, tentunya sangat diperlukan suatu sistem yang menjaga agar data tersebut terjamin kerahasiaan dan keutuhannya. file yang tidak terjamin kerahasiaannya akan dapat dengan mudah dimanfaatkan atau diambil oleh orang yang tidak berhak. Dalam pengiriman data yang melalui jaringan, diperlukan suatu metode agar data tersebut tidak hilang atau utuh sampai tujuan. Dalam penyimpanan data diperlukan suatu keamanan agar data yang disimpan tidak dapat dibuka, dibaca bahkan diambil oleh orang yang bukan haknya untuk mencoba membukanya.

Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. (*Cryptography is the art and science of keeping messages secure*) *Crypto* berarti *secret* (rahasia) dan graphy berarti writing (tulisan). Para pelaku atau praktisi kriptografi disebut cryptographers. Sebuah algoritma kriptografik (*cryptographic* algorithm), disebut cipher, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat. Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut plaintext) menjadi pesan yang tersembunyi (disebut ciphertext) adalah enkripsi (*encryption*). Ciphertext adalah pesan yang sudah tidak dapat dibaca dengan mudah. Proses sebaliknya, untuk mengubah ciphertext menjadi plaintext, disebut dekripsi (decryption). terminologi yang lebih tepat untuk proses ini adalah decipher.

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi data anda disandikan (*encrypted*) dengan menggunakan sebuah kunci (key). Untuk membuka (*decrypt*) data tersebut digunakan juga sebuah kunci yang sama dengan kunci untuk mengenkripsi (untuk kasus *private key cryptography*) atau dengan kunci yang berbeda (untuk kasus public key *cryptography*). Algoritma dari enkripsi adalah fungs-ifungsi yang digunakan untuk melakukan fungsi enkripsi dan dekripsi. Algoritma yang digunakan menentukan kekuatan dari enkripsi, dan ini biasanya dibuktikan dengan basis matematika. Dalam system keamanan data dikenal sebuah metode enkripsi yang mempunyai kode-kode

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 1, September 2020
e-ISSN 2685-998X
DOI 10.30865/json.v2i1.2457

pengamanan untuk mengacak data dan juga mempunyai kode- kode untuk mengembalikan data yang teracak ke data yang sebenarnya. Salah satu metoda yang akan dibahas pada penelitian ini adalah Algoritma venigmare cipher dan vernam cipher.

Venigmare cipher adalah diambil dari salah satu nama mesin yang dipakai jaman dahulu untuk keperluan rahasia militer Jerman yang diberi nama Enigma Machine. yaitu ada rotor yang akan menyebabkan susunan substitusi huruf akan berubah setiap selesai melakukan enkripsi satu huruf. Maka pada algoritma Venigmarè yang dirancang sistem kerja ini digunakan, ketika satu huruf selesai dienkripsi dengan sebuah kunci maka baris dimana cipherteks didapatkan akan digeser (wrapping) ke kanan.

Vernam cipher merupakan algoritma kriptografi yang ditemukan oleh Mayor J. Maugborne dan G. Vernam. Algoritma Vernam cipher diadopsi dari one time pad cipher, dimana dalam hal ini karakter diganti dengan bit (0 atau 1). Dengan kata lain, vernam cipher merupakan versi lain dari one-time pad cipher. Algoritma kriptografi vernam cipher merupakan algoritma kriptografi berjenis symmetric key. Kunci yang digunakan untuk melakukan enkripsi dan dekripsi menggunakan kunci yang sama. Dalam melakukan proses enkripsi, algoritma vernam cipher menggunakan cara stream cipher dimana cipher berasal dari hasil operasi XOR antara bit plainteks dan bit key

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi berasal dari Bahasa Yunani, crypto dan graphia.Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim kesuatu tempat ke tempat lainKriptoggrafi berfungsi agar data yang dikirim aman dari gangguan orang yang tidak bertanggung jawab, yang disembunyikan menggunakan algoritma kriptografi.

2.2 Algoritma *Venigmarè Cipher*

Pada Vigenère biasa, enkripsi satu huruf plaintext pada satu huruf kunci yang sama akan mengakibatkan satu huruf ciphertext yang sama. Hal ini lah yang mengakibatkan teknik analisis frekuensi masih dapat dilakukan pada Vigenère cipher cukup dengan mengetahui panjang kunci. Untuk itu dibutuhkan variasi yang mengakibatkan satu huruf palinteks jika di enkripsikan dengan satu huruf kunci yang sama akan menghasilkan hasil yang berbeda[3].

Berdasarkan dalam cara kerja mesin enigma, yaitu ada rotor yang akan menyebabkan susunan substitusi huruf akan berubah setiap selesai melakukan enkripsi satu huruf. Maka pada algoritma Venigmarè yang dirancang ini sistem kerja ini digunakan. Ketika satu huruf selesai dienkripsi dengan sebuah kunci maka baris dimana ciphertext didapatkan akan digeser (wrapping) ke kanan. Jadi, pada kondisi awal jika kita melakukan enkripsi huruf I dengan kunci I, sehingga menghasilkan ciphertext Q.

Jika dituliskan dalam program, maka metode ini selain menggunakan formula umum (P;K; C; E;D) perlu adanya tambahan untuk menyimpan informasi tabel hasil enkripsi. Akibatnya kita perlu menambahkan satu struktur data baru berupa array of char sebanyak 26 huruf, yang tiap index menyatakan jumlah pergeseran pada tiap baris. Jika diformulasikan maka algoritma untuk enkripsi akan didapatkan:

$$\textbf{Enkripsi } C_i \equiv (P_i + k_i + B_k) \bmod 26 \qquad (1)$$

Dimana C adalah ciphertext, P adalah plaintext, K adalah kunci, dan B adalah informasi pergeseran baris pada kunci yang bersesuaian. Dan setelah selesai enkripsi satu huruf, informasi tabel perlu di-increment. Sehingga $B_k = B_k + 1$.

Dan untuk proses dekripsi akan didapatkan formula yang merupaka balikan dari formula enkripsi yaitu :

$$\textbf{Dekripsi } P_i \equiv (C_i + k_i + B_k) \bmod 26 \qquad (2)$$

Untuk setiap selesai melakukan dekripsi maka nilai dari B akan di-decrement. Sehingga $B_k = B_k - 1$. Tentunya algoritma ini masih dapat divariasikan juga dengan variasi yang digunakan pada Vigenère cipher sebelumnya seperti running-key, one-time pad, dan gronsfeld cipher serta ekspansi dari alfabet menjadi ASCII table [3].

2.3 Algoritma *Vernam Cipher*

Vernam cipher adalah jenis algoritma enkripsi simetri. *Vernam cipher* dapatdibuat sangat cepat sekali, jauh lebih cepat dibandingkan dengan algoritma *block cipher*yang manapun. Algoritma *block cipher* secara umum digunakan untuk unit *plaintext*yang besar sedangkan *stream cipher* digunakan untuk blok data yang lebih kecil,biasanya ukuran bit. Proses enkripsi terhadap *plaintext* tertentu dengan algoritma *blockcipher* akan menghasilkan *ciphertext* yang sama jika kunci yang sama digunakan. Dengan *stream cipher*, transformasi dari unit *plaintext* yang lebih kecil ini berbedaantara satu dengan lainnya, tergantung pada kapan unit tersebut ditemukan selamaproses enkripsi.Satu *vernam cipher* menghasilkan apa yang disebut suatu *keystream* (suatubarisan bit yang digunakan sebagai kunci). Proses enkripsi dicapai denganmenggabungkan *keystream* dengan *plaintext* biasanya dengan operasi *bitwise XOR.*

Pembentukan *keystream* dapat dibuat independen terhadap *plaintext* dan *ciphertext*,menghasilkan *synchronous stream cipher*, atau dapat dibuat tergantung pada data danenkripsinya, dalam hal mana *stream cipher* disebut sebagai *self-synchronizing*.Kebanyakan bentuk *stream cipher* adalah *synchronous stream*

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 1, September 2020
e-ISSN 2685-998X
DOI 10.30865/json.v2i1.2457

cipher.Konsentrasi dalam *stream ciphers* pada umumnya berkaitan dengan sifat sifatteoritis yang menarik dari *one-time pad*. Suatu one-time pad, kadang-kadang disebut*Vernam cipher*, menggunakan sebuah string dari bit yang dihasilkan murni secara*random* (Kromodimoeljo, 2009). *Keystream* memiliki panjang sama dengan pesan*plaintext*; string random digabungkan dengan menggunakan *bitwise* XOR dengan*plaintext* untuk menghasilkan *ciphertext*. Karena *keystream* seluruhnya adalah random,walaupun dengan sumber daya komputasi tak terbatas seseorang hanya dapat menduga *plaintext* jika melihat *ciphertext*. Metode *cipher* seperti ini disebut memberikankerahasiaan yang sempurna (*perfect secrecy*). Metode *vernam cipher* yang umumdigunakan adalah RC4. Satu hal yang menarik bahwa mode operasi tertentu dari suatu*block cipher* dapat mentransformasikan secara efektif hasil operasi tersebut ke dalamsatu *keystream* generator dan dalam hal ini, *block cipher* apa saja dapat digunakansebagai suatu *stream cipher*; seperti dalam DES, CFB atau OFB. Akan tetapi, *vernamciphers* dengan desain khusus biasanya jauh lebih cepat. *Cipher*teks diperoleh dengan melakukan penjumlahan *modulo* 2 satu bitplainteks dengan satu bit kunci:

$$\textbf{Enkripsi } C_i \equiv (P_i + k_i) \bmod 26 \quad (3)$$

Dimana, P_i adalah bit plainteks, k_i adalah bit kunci, dan C_i adalah bit*cipher*teks. Plainteks diperoleh dengan melakukan penjumlahan *modulo* 2 satu bit*cipher*teks dengan satu bit kunci:

$$\textbf{Dekripsi } P_i \equiv (C_i + k_i) \bmod 26 \quad (4)$$

Aliran-bit-kunci dibangkitkan dari sebuah pembangkit yang dinamakanpembangkit aliran-bit-kunci (*keystream generator*). Aliran-bit-kunci (sering dinamakan*running key*) di-XOR-kan dengan aliran bit-bit plainteks, *p*1, *p*2, …, *pi*, untukmenghasilkan aliran bit-bit *cipher*teks:

$$\textbf{Enkripsi } C_i \equiv (P_i \oplus k_i) \bmod 26 \quad (5)$$

Di sisi penerima, bit-bit *cipher*teks di-XOR-kan dengan aliran-bit-kunci yangsama untuk menghasilkan bit-bit plainteks:

$$\textbf{Dekripsi } P_i \equiv (C_i \oplus k_i) \bmod 26 \quad (6)$$

Merancang pembangkit bit-aliran-kunci yang bagus cukup sulit karenamembutuhkan pengujian statistik untuk menjamin bahwa keluaran dari pembangkit tersebut sangat mendekati barisan acak yang sebenarnya.

3. HASIL DAN PEMBAHASAN

Pada Proses Analisa Metode dalam implementasi cara dan bentuk penggunaan metode, analisa sangat penting dalam membuat hal procedur enkripsi file. Analisa Metode sangat langkah awal dalam Memahami Pembuatan perancangan aplikasi yang akan dikerjekan sehingga masalah perancangan dapat segera terselesaiakan.

3.1 Penerapan Algoritma Venigmare Cipher

Penggunaa algoritma Venigmare adalah sama halnya dengan metode vegenare dimana algoritma Venigmare memiliki ukuran sedikit legih panjang dengan metode Vegenare. Berikut contoh nya : Pemecahan Kata GREEN CAMPUS dengan Kunci POLTEK
Termasuk ke dalam cipher abjad-majemuk (polyalpabetic substitution cipher). Vigènere Cipher menggunakan Bujursangkar Vigènere untuk melakukan enkripsi. Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar Cipher (A = 0, B = 1, C = 2, …., Z = 25)

Tabel 1. Cipher abjad-majemuk

A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8
J	K	L	M	N	O	P	Q	R
9	10	11	12	13	14	15	16	17
S	T	U	V	W	X	Y	Z	
18	19	20	21	22	23	24	25	

Sehingga menghasilkan tabel sebagai berikut

Tabel 1. Hasil Venigmare Chipher

Plaintext	**G**	**R**	**E**	**E**	**N**	**C**	**A**	**M**	**P**	**U**	**S**
Indeks (P)	**6**	**17**	**4**	**4**	**13**	**6**	**0**	**12**	**15**	**20**	**18**
Kunci	B	U	D	I	D	A	R	M	B	U	D
Indeks (K)	1	20	3	8	3	0	17	12	1	20	3
P+K	**7**	**37**	**7**	**12**	**16**	**6**	**17**	**24**	**16**	**40**	**21**
Cipertext	H	L	H	M	Q	G	R	Y	Q	O	V

Dengan kata Hasil : HLHMQGRYQOV

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 1, September 2020
e-ISSN 2685-998X
DOI 10.30865/json.v2i1.2457

3.2 Penerapan Algoritma Vernam Cipher

Metode Vernam Cipher merupakan algoritma berjenis symmetric key kunci yang digunakan untuk melakukan enkripsi dan dekripsi yang menggunakan kunci yang sama. Dalam proses enkripsi, algoritma Vernam Cipher menggunakan cara stream cipher dimana cipher berasal dari hasil XOR antara bit plaintext dan bit key, sedangkan permutasi biner dilakukan dengan membalikan kode biner pada setiap karakter.

Enkripsi dapat digambarkan sebagai penjumlahan *modulo* 26 dari satu karakter plainteks dengan satu karakter kunci *one time pad* :

ci = (pi + ki) mod 26

keterangan :

pi : karakter plainteks

ki : karakter kunci

ci : karakter *Cipher*tek

Deretan Abjad

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext: GREEN KAMPUS
Ki Text : BUDIDARMA
Cara dekripsi :

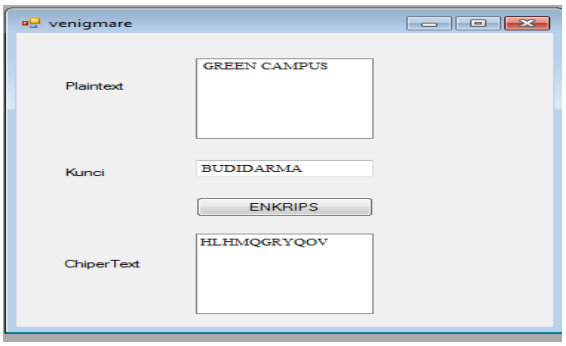
Plaintext: GREEN KAMPUS	=	6 17 4 4 13 10 0 12 15 20 18
ki Text : BUDIDARMA	=	1 20 3 8 3 0 17 12 1 20 3
		7 37 7 12 16 6 17 24 16 40 21

Hasil : HLHMQGRYQOV
Sedangkan dekripsi:

Chipertext : HLHMQGRYQOV	=	7 37 7 12 16 6 17 24 16 40 21
Key : BUDIDARMA		1 20 3 8 3 0 17 12 1 20 3
		6 17 4 4 13 10 0 12 15 20 18
Plaintext :		GREEN KAMPUS

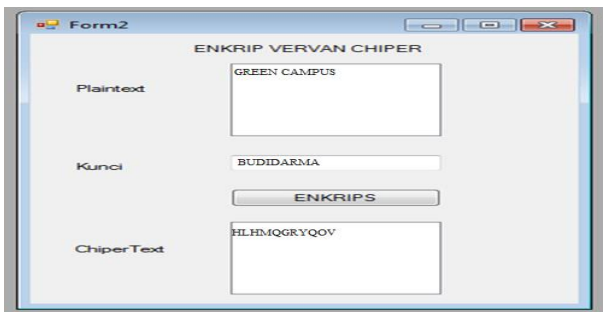
3.3 Implementasi

Tampilan Enkripsi Venigmare dapat dilakukan dengan cara memilih menu “Enkripsi dan memilih Venigmare” pada menu utama. Menu ini sebagai menu untuk proses enkrip data atau file. Tampilan menu enkripsi ini dapat dilihat pada gambar 1. seperti dibawah ini:



Gambar 1. Venigmare Chiper

Tampilan Enkripsi Vernam Chiper dapat dilakukan dengan cara memilih menu “Enkripsi dan memilih Vernam” pada menu utama. Menu ini sebagai menu prose enkripsi metode vernam chiper. Tampilan menu ini dapat dilihat pada gambar 2. seperti dibawah ini :



Gambar 2. Tampilan Vernam Chiper

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 1, September 2020
e-ISSN 2685-998X
DOI 10.30865/json.v2i1.2457

4. KESIMPULAN

Dari penyelesaian penelitian ini penulis dapat mengambil kesimpulan sebagai berikut :

1. Dengan adanya proses pengamanan data, penggunaan data dapat diilakukan dengan baik dan aman.
2. Dengan menerapkan *Algoritma Venigmare* dan *Vernam Chiper* dapat Mengenkrip data dengan cepat dan baik.
3. Dengan adanya pengamanan data ini dapat digunakan jika pengguna menerapkan dengan benar dan dapat diterapkan dalam membantu orang banyak baik perseorangan maupun organisasi.

REFERENCES

[1] J. Enterprise, Rahasia Manajemen File Refensi Praktis Seputar File Dan Manajemen Data, Jakarta : Elex Media Komputindo, 2010.
[2] U.S. Respationo, "Venigmarè Cipher dan Vigenère Cipher", ITB, pp.4-5, 2009
[3] C.A. Sari, "Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting", Journal of Applied Intelligent System, Vol.1, No. 3, 179-190, 2016.
[4] E. Irwansyah dan J.V. Moniaga, Pengantar Teknologi Informasi, Yogyakarta : Deepublish, 2014.
[5] A. Nugroho, Rekayasa Perangkat Lunak Berorientasi Objek Dengan Metode USDP (unified Software Development Process), Yogyakarta : Andi, 2010.
[6] D. Ariyus, Pengantar Ilmu Kriptografi: Teori Analisis Dan Implementasi, Yogyakarta : Andi, 2008.