MODIFIKASI METODE HILL CIPHER DAN VERNAM CIPHER MENGUNAKAN KODE ADMINISTRASI DAN PAJAK

Agatha Deolika

Magister Teknik Informatika, Universitas Amikom, Yogyakarta
Jl. Ring Road Utara, Condong Catur, Sleman, Yogyakarta
agatha.deolika@students.amikom.ac.id.

Abstract **-** Access to information in the current era is easily accessible and can be accessed anywhere and anytime. Our data can be accessed in public or confidential, for confidential data the very need for security is taken or manipulated by parties who are not responsible. One way to support data is by disguising data to codes that cannot be done using cryptography. In cryptography that contains many algorithms, this study combines the Hill cipher and Vernam Cipher methods that facilitate using the state administration code and Tax. The results of this study are the hill cipher conversion method with the state administration code and the regional abbreviation code in Indonesia, after which it is combined with the vernam cipher method which also combines with the tax value. The results of encryption with this algorithm combination type .txt file that contains a combination of letters, numbers, and symbols. Testing is done by comparing the process of several file types in terms of speed and the amount of data needed at the time of encryption and description.
Keywords**:** Vernam Cipher, Hill Cipher, Kriptografi.

Abstrak **-** Akses informasi pada era sekarang ini sangatlah mudah dan dapat diakses dimanapun dan kapanpun. Bahkan kita dapat mengakses data yang dipublish ataupun yang bersifat rahasia, untuk data yang bersifat rahasia sangat perlunya keamanan karena rentan diambil atau dimanipulasi oleh pihak - pihak yang tidak bertanggung jawab. Salah satu cara untuk mengamankan data dengan menyamarkan data ke kode - kode yang tidak bermakna yang dapat dilakukan menggunakan kriptografi. Dalam kriptografi terdapat banyak algoritma, pada penelitian ini mengkombinasikan metode Hill cipher dan Vernam Cipher yang dimodifikasi menggunakan kode administrasi negara dan Pajak. Hasil dari penelitian ini adalah memodifikasi metode hill cipher dengan kode administrasi negara dan kode singkatan daerah di Indonesia, setalah itu dikombinasikan dengan metode vernam cipher yang dimodifikasi juga dengan nilai pajak. Hasil dari enkripsi dengan kombinasi algoritma ini bertipe file .txt yang berisi kombinasi huruf, angka, dan symbol. Pengujian dilakukan dengan membandingkan proses beberapa jenis file dari segi kecepatan serta jumlah data yang diproses pada saat enkripsi dan deskripsi.
Kata Kunci**:** Vernam Cipher, Hill Cipher, Kriptografi.

I. PENDAHULUAN

Pada era sekarang ini pemanfaatan teknologi informasi sangatlah diperlukan. Salah satunya sebagai media transfer data ataupun penyimpanan data, sehingga memudahkan orang dalam mengakses suatu informasi. Dampak dari proses tersebut yaitu pada keamanan data atau pesan yang menggunakan media tersebut. Salah satu cara yang dapat digunakan untuk menjaga kerahasiaan data tersebut adalah dengan menyamarkan menjadi kode-kode yang tidak bermakna, yang dapat dilakukan dengan menggunakan kriptografi. Kriptografi adalah ilmu yang mempelajari bagaimana menjaga data tetap aman saat melakukan proses transfer data atau penyimpanan data agar tidak mengalami gangguan dari pihak ketiga, yang bertujuan untuk menjaga kerahasiaan. Didalam kriptografi terdapat dua konsep utama yaitu enkripsi dan deskripsi [1].

Ada beberapa algoritma atau metode yang dapat digunakan dalam proses kriptografi seperti metode Vernam Cipher, Hill Cipher, dan lain sebagainya.

Metode Vernam Cipher adalah jenis algoritma enkripsi simetri, Vernam cipher dapat dibuat sangat cepat sekali, jauh lebih cepat dibandingkan dengan algoritma block cipher yang manapun. Metode ini memungsikan boolean ekslusif (Ex-OR dan Ex-Nor) [2]. Sedangkan metode Hill Cipher adalah cipher simetris klasik berdasarkan transformasi matriks. Metode ini memiliki beberapa keuntungan termasuk ketahanan terhadap analisis frekuensi dan implicity karena metode ini menggunakan perkalian matriks dan inversi untuk enkripsi dan dekripsi [3].

Pada penelitian Selviana yang berjudul "Modifikasi Algoritma Hill Cipher dan Twofish Menggunakan Kode Wilayah Telepon" mengatakan, modifikasi algoritma hill cipher dan twofish, proses enkripsi dan dekripsi file sangat bergantung dengan besarnya ukuran file, dimana ukuran file akan mempengaruhi kecepatan dan jumlah data yang diproses. Semakin besar ukuran file, maka akan semakin lama proses enkripsi dan dekripsinya [4]. Farmandar, Mina and Alexander G. Chefranov pada penelitiannya mengatakan bahwa metode Hill Cipher dalam pembacaan sandi relatif mudah atau rentan

terhadap serangan pengenalan plaintext-ciphertext karena linearitas [5].

Eko Hari Rachmawanto dalam penelitiannya mengatakan bahwa metode Vernam Cipher membuktikan bahwa dapat mengacak file dengan aman dan tidak menimbulkan kecurigaan pada pihak lain. Pada file hasil, tidak menimbulkan efek yang dapat merusak ataupun mengganggu kinerja file sebelumnya [6].

Algoritma hill cipher dan vigenere cipher adalah salah satu metode dari beberapa metode yang digunakan untuk keamanan data, Jika kedua algoritma diatas dikombinasikan dan di modifikasi dalam sebuah sistem keamanan data, maka akan sulit pihak-pihak yang tidak bertanggung jawab untuk memanipulasi data dan bila dibandingkan dengan hanya menggunakan satu algoritma saja, kombinasi 2 algoritma dan modifikai jauh lebih bagus. Penelitian ini bertujuan untuk membuat suatu modifikasi algoritma kriptografi dan mengkombinasikan 2 metode yaitu Hill cipher dan Vernam Cipher yang akan sedikit dimodifikasikan menggunakan kode wilayah administrasi, singkatan nama provinsi, dan juga menambahkan rumus PPH dan PPN 11,5%.

Penelitian ini diharapkan nantinya dapat memberikan alternatif algoritma yang lebih baik dari segi kecepatan enkripsi serta kerumitan dalam pemecahan sandi. Pengujian dilakukan dengan membandingkan beberapa jenis data yang dienkripsi dengan algoritma tersebut serta bagaimana kecepatan enkripsi menggunakan modifikasi algoritma ini.

II. LANDASAN TEORI

A. *Kode Wilayah Administrasi dan Singkatan Nama Provinsi*

Pada penelitian ini menggunakan kode wilayah administrasi yang menggunakan Peraturan Menteri Dalam Negeri Nomor 72 Tahun 2019 Tentang Perubahan atas Peraturan Menteri Dalam Negeri Nomor 137 Tahun 2017 tentang Kode dan Data Wilayah Administrasi Pemerintahan. Sedangkan untuk singkatan nama Provinsi menggunakan standar ISO 3166-2:2007 yang diterbitkan oleh Badan Standarisasi Nasional (BSN).

Tabel 1. Daftar Kode Wilayah Adminustrasi

No	Kode	Kabupaten/Kota	Modifikasi
1	61.11	KAB. KAYONG UTARA	6-1-1-1
2	62.11	KAB. PULANG PISAU	6-2-1-1
3	63.11	KAB. BALANGAN	6-5-1-1
4	64.11	KAB. MAHAKAM ULU	6-4-1-1
5	71.11	KAB. BOLAANG MONGONDOW SELATAN	7-2-1-1
6	73.11	KAB. BARRU	7-4-1-1
7	13.11	KAB. SOLOK SELATAN	1-4-1-1
8	16.11	KAB. EMPAT LAWANG	1-6-1-1

B. *Pajak PPH PPN*

Pada penelitian ini menggunakan PPH pasal 22 yang dikenakan 1,5% dan juga menggunakan PPN 10% yang diatur pada Undang-Undang Dasar No.42, Tahun 2009, pasal 7. Maka dari itu PPH dan PPN akan dijumlahkan menghasilkan 11,5%.

C. *Definisi Hill Cipher*

Metode Hill Cipher adalah cipher simetris klasik yang memecah plaintext menjadi blok-blok ukuran m dan kemudian mengalikan setiap blok oleh sebuah kunci matriks m x m untuk menghasilkan ciphertext [3].

Teknik Hill Cipher adalah aritmatika modulo terhadap matriks. Dalam penerapannya, Hill Cipher menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada Hill Cipher adalah matriks n x n dengan n merupakan ukuran blok. Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible, yaitu memiliki inverse K-1 sehingga:

Keterangan:
K = Kunci
K-1 = Invers Kunci
I = Matriks Identitas

D. *Definisi Vernam Cipher*

Menurut Sadikin, sandi vigenere merupakan sistem sandi polialfabetik mengenkripsikan sekaligus sebuah teks yang terdiri dari beberapa huruf. Sandi vigenere menggunakan subtitusi dengan fungsi shift [7]. Sedangkan menurut Ariyus, pada teknik subtitusi vigenere setiap ciphertext bisa memiliki banyak kemungkinan plaintextnya. Teknik ini bisa dilakukan oleh dua cara yaitu : angka dan huruf. [8] Algoritma block cipher secara umum digunakan untuk unit plaintext yang besar sedangkan stream cipher digunakan untuk blok data yang lebih kecil, biasanya ukuran bit [9].

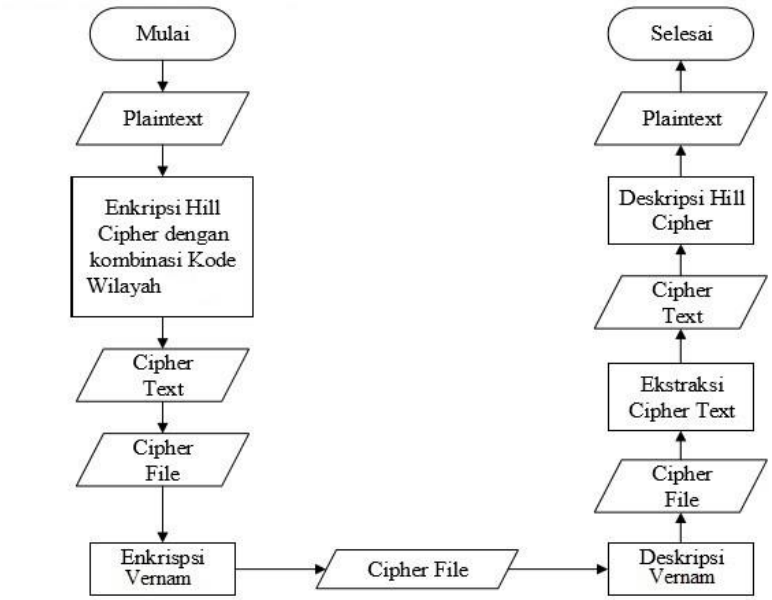
III. METODE PENELITIAN

Penelitian yang akan dilakukan berjenis penelitian eksperimen. Penelitian dilakukan menggunakan dataset yang didapatkan dari ekperimen sendiri. Penelitian ini menggunakan data teks yang terdapat pada file .txt yang beragam macam jumlah ukuran filenya. Metode yang digunakan dalam penelitian ini adalah analisisi kecepatan waktu algoritma meekseskusi data.

A. *Tahap Penelitian*

Dalam pengerjaan penelitian ini diperlukan langkah-langkah kegiatan penelitian, dapat dilihat alur penelitian pada Gambar 1. Langkah-langkah tersebut adalah sebagai berikut :

1. Menginput Plaintext pada system.
2. Enkripsi Plaintext menggunakan Hill Cipher dengan kombinasi kode wilayah administrasi dan kode singkatan provinsi.
3. Hasil enkripsi dari hill cipher akan menjadi plaintext vernam dan di enkripsi menggunakan kombinasi rumus PPH dan PPN.
4. Untuk proses Deskripsi akan dilakukan sebaliknya, mulai dari deskripsi vernam cipher.
5. Hasil dari vernam ciper akan di deskripsi menggunakan metode hill cipher dan akan mengasilkan hasilciper text atau ciper file.



Gambar 1. Alur Penelitian

IV. HASIL DAN PEMBAHASAN

A. Enkripsi

Mengenkripsi plaintext “SAYA CINTA INDONESIA” dengan matriks kunci 2x2 berdasarkan kode wilayah kota/kabupaten.

Tabel, 2

KEY	MATRIX 2X2			KEY	MATRIX 2X2	
K1	6	1		K5	7	1
	1	1			1	2
K2	6	1		K6	7	1
	1	2			1	4
K3	6	1		K7	1	1
	1	5			1	4
K4	6	1		K8	1	1
	1	4			1	6

Langkah pertama mengubah plaintext menjadi angka berdasarkan dengan menggunakan tabel berikut.

Tabel. 3

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Sehingga plaintext menghasilkan tabel. 3.

Tabel. 4

S	**A**	**Y**	**A**	**C**	**I**	**N**	**T**	**A**	**I**	**N**	**D**	**O**	**N**	**E**	**S**	**I**	**A**
18	0	24	0	2	8	13	19	0	8	13	3	14	13	4	18	8	0

Langkah selanjutnya membagi menjadi perblok dengan 2 angka pada masing-masing blok, Jika data berjumlah ganjil maka digenapkan dengan menambahkan angka 26. Setelah itu masing-masing blok akan di enkripsi dengan menggunakan algoritma Hill Cipher. Berikut hasil chipertext:

Tabel. 5

No	**Matrix K**		**Matrik Blok**			**Perkalian**	**Mod 34**	**Kode Provinsi**
1	6	1	*	18	=	108	6	SS
	1	1		0		18	18	NT
2	6	1	*	24	=	144	8	LA
	1	2		0		24	24	SA
3	6	1	*	2	=	20	20	KT
	1	5		8		42	8	LA
4	6	1	*	13	=	97	29	SG
	1	4		19		89	21	KS
5	7	1	*	0	=	8	8	LA
	1	2		8		16	16	BA
6	7	1	*	13	=	94	26	ST
	1	4		3		25	25	GO
7	1	1	*	14	=	27	27	SN
	1	4		13		66	32	PA
8	1	1	*	4	=	22	22	KI
	1	6		18		112	10	JK
9	6	1	*	8	=	48	14	YO
	1	1		0		8	8	LA

Setelah mendapatkan chipertext “SSNTLASAKTLASGKSLABASTGOSNPAKIJKYOLA” maka akan dilakukan proses metode vernam chipper. Pada metode ini menggunakan kunci seperti pada tabel 5 berikut:

Tabel. 6

K	**A**	**L**	**T**	**E**	**N**	**G**
10	0	11	19	4	13	6

Proses pertama pada metode ini melakukan enkripsi vernam chipper dan setelah itu dikombinasikan dengan perhitungan PPH+PPN.

Tabel. 7

18	**18**	**13**	**19**	**11**	**0**	**18**	**0**	**10**	**19**		**0**
10	0	11	19	4	13	6	10	0	11	**…**	10
28	18	24	38	15	13	24	10	10	30		10
MOD 26											
2	18	24	12	15	13	24	10	10	4		10
200	1800	2400	1200	1500	1300	2400	1000	1000	400		1000
23	207	276	138	172,5	149,5	276	115	115	46		115
C	S	Y	M	P	N	Y	K	K	E	…	K
23C	207S	276Y	138M	172,5P	149,5N	276Y	115K	115K	46E		115K
23C	207S	276Y	138M	172~5P	149`5N	276Y	115K	115K	46E		115K

Plaintext “Saya Cinta Indonesia” menghasilkan chipertext
“**23C207S276Y138M172~5P149`5N276Y115K115K46E46E46E57!5F138M230U207S253W218@5T57#5F149$5N276Y34%5D69G287^5Z126&5L195*5R23C69G230U92I230U34(5D23C11)5B195_5R115K**”

B. Deskripsi

Dilakukan proses deskripsi menggunakan vernam chipper berdasarkan plaintext diatas dapat dilihat pada tabel 7, dan setelah itu melakukan proses hill chipper pada tabel 8 dan table 9.

Tabel. 8

2	**18**	**24**	**12**	**15**	**13**	**24**	**10**	**10**	**4**		**10**
10	0	11	19	4	13	6	10	0	11	…	10
-8	18	13	-7	11	0	18	0	10	-7		0
MOD 26											
18	18	13	19	11	0	18	0	10	19	…	A
S	S	N	T	L	A	S	A	K	T		10

1	SS	6	6	1		5		1	-1	=	7	27	=	18	S
	NT	18	1	1		7		-1	6		27	8		0	A
2	LA	8	6	1		11		2	-1	=	28	3	=	24	Y
	SA	24	1	2		31		-1	6		3	16		0	A

Tabel. 9

C. Pengujian

Hasil uji coba menggunakan beberapa data untuk mengukur kecepatan proses enkripsi dan deskripsi dari modifikasi algoritma pada penelitian ini dapat dilihat pada tabel berikut.

Tabel. 10

No	**Nama Data**	**Ukuran Asli (byte)**	**Enkripsi**		**Deskripsi**	
			Ukuran Data	**Waktu**	**Ukuran Data**	**Waktu**
1	Data 1	534	754	1.02	752	1.02
2	Data 2	1076	2235	3.45	2230	3.49
3	Data 3	13.012	19.454	4.43	19.447	4.53
4	Data 4	237.441	416.286	4.97	416.282	5.23
5	Data 5	309.986	587.654	6.43	587.643	6.89

V. KESIMPULAN

Adapun kesimpulan yang diperoleh adalah:

1. Dengan memodifikasi metode dapat membuat keamanan dan panjang data berubah yang membuat keamanan data lebih aman dengan kombinasinya.
2. Adanya perubahan ukuran data dikarenakan satu huruf dari plaintext dapat menghasilkan 3 atau lebih karakter chipertext yang mengakibatkan ukuran data hampir 2 kali lipat lebih besar.

VI. SARAN

Sarannya untuk penelitian selanjutnya agar dilakukan penelitian menggunakan kombinasi yang sama untuk tipe data seperti suara, gambar dan video, dan juga ditambahkan proses steganografi.

DAFTAR PUSTAKA

[1] Dony Ariyus, Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi, Andi Offset, 2008.
[2] *Ryabko, Boris, The Vernam Cipher is Robust to Small Deviations from Randomness, 2013.*
[3] Magambar, Kondwani, et al., Variable-length Hill Cipher with MDS Key Matrix, 2012.
[4] Selviana Yunita, Patmawati Hasan, Dony Ariyus., Modifikasi Algoritma Hill Cipher dan Twofish Menggunakan Kode Wilayah Telepon, Jurnal

Ilmiah SISFOTENIKA, Vol. 9, No. 2, Juli 2019, 2019.

[5] Farmamdar, Mina and Alexander G. Chefranov., Investigation of Hill Cipher Modification Based on Permutation and Iteration, International Journal of Computer Science and Information Security (IJCSIS), Vol. 10, No. 9, September 2012, 2012.

[6] Eko Hari Rachmawanto, Kriptografi Vernam Cipher Untuk Mencegah Pencurian Data Pada Semua Ekstensi File, Seminar Nasional Multi Disiplin Ilmu Unisbank, 2016.

[7] Sadikin, Kriptografi untuk Keamanan Jaringan. Andi , Yogyakarta, 2012.

[8] Ariyus, Kriptografi Keamanan Data dan Komunikasi. Andi, Yogyakarta, 2006.

[9] Stinson, D. Cryptography Theory and Practice. Florida: CRC Press, 1995.