Enkripsi Data Berupa Teks Menggunakan Metode Modifikasi *Vigenere Cipher*

Hendro Eko Prabowo
Jurusan Teknik Elektro
Universitas Negeri Semarang
Semarang, Indonesia
Email : hendro.prabowo15@gmail.com

Arimaz Hangga
Jurusan Teknik Elektro
Universitas Negeri Semarang
Semarang, Indonesia
Email : Ari.maz.hangga@gmail.com

Abstrak—Tindakan pencurian data sering terjadi pada aplikasi maupun jaringan komunikasi khususnya data berupa teks. Penyebab utama terjadi tindakan pencurian data berupa teks adalah belum adanya prosedur pengamanan. Terdapat beberapa cara prosedur pengamanan, penyandian atau enkripsi data merupakan salah satu teknik keamanan data yang sering digunakan. Penelitian ini bertujuan untuk memberikan prosedur pengamanan pada data teks dengan metode algoritma modifikasi *vigenere cipher*. Hasil simulasi menunjukkan bahwa algoritma modifkasi *vigenere cipher* tidak ada perulangan kata sehingga kunci enkripsi tidak mudah diprediksi. Akan tetapi pada algoritma *vigenere cipher* terlihat bahwa terdapat perulangan kata pada hasil enkripsi dengan peluang terbesar informasi dapat diprediksi sebesar 74,07 %. Kelebihan modifikasi algoritma *vigenere cipher* dalam penelitian ini adalah hasil enkripsi tidak memiliki pola perulangan huruf atau kata.

Kata kunci—penyandian, *vigenere cipher*, data teks.

Abstract—The stealing of data often occurs on the application and communications networks in data of text. The main cause of the stealing data of text is lack of security procedures. There are many security procedures, encryption data is one of security techniques used often. In this research aims to give security procedures in data of text by modification of vigenere cipher algorithm method.The result indicate that modification of vigenere cipher algorithm method there is no looping letter so that encryption key is not easy predicted. However the vigenere cipher algorithm have looping letter in the results of encryption with the largest opportunities of information can be predicted 74,07%. The advantages of modification of vigenere cipher algorithm in this research is the encryption result have not looping patterns letter or word.

Keywords—encryption, vigenere cipher, data of text.

I. PENDAHULUAN

Teknik keamanan data terus dikembangkan untuk meminimalkan pencurian data. Peningkatan prosedur pengamanan data sering dikembangkan agar data tidak dapat dicuri. Penyandian data dapat diterapkan untuk meningkatkan pengamanan data berupa teks. Penyandian atau enkripsi data merupakan proses pengubahan informasi data agar data tidak terbaca. Hasil dari enkripsi berupa informasi yang disandikan (*cipher text*) sedangkan proses pembalikan sandi untuk mendapatkan informasi disebut dekripsi [1]. Algoritma kriptografi digunakan pada proses enkripsi maupun deskripsi. Pada umumnya algoritma kriptografi dibedakan menjadi dua jenis, yaitu kriptografi kunci simetris (*symmetric key cryptography*) dan kriptografi kunci tidak simetris (*asymmetric key cryptgraphy)* [2].

Kriptografi kunci simetris merupakan algoritma kriptografi yang menggunakan kunci yang sama dalam proses enkripsi dan dekripsi. Sedangkan pada kriptografi kunci tidak simetris merupakan algoritma yang menggunakan dua kunci yang berbeda yaitu *private key* dan *public key*. *Public key* adalah kunci yang digunakan untuk enkripsi. *Private key* adalah kunci yang digunakan untuk mendeskripsi *cipher text* untuk menadapatkan informasi. *Private key* hanya diketahui oleh pendekripsi *cipher text*.

Vigenere cipher adalah salah satu contoh metode kriptografi kunci simetris dengan tingkat keamanan kunci yang lebih sulit dipecahkan. Hal ini disebabkan algoritma dari *vigenere cipher* merupakan bentuk sederhana dari subtitusi polialfabetik dengan kunci enkripsi berupa huruf [3]. Dengan adanya tingkat keamanan data yang rendah pada data berupa teks maka penelitian ini diharapkan dapat memberikan prosedur pengamanan pada data berupa teks dengan modifikasi *vigenere cipher*.

II. METODE PENELITIAN

Pada penelitian ini menggunakan metode *vigenere cipher* dan *caesar cipher*. *Caesar cipher* digunakan sebagai pembentuk kunci awal untuk membentuk kunci baru. Kunci masukan dari pengguna akan dienkripsi menggunakan *caesar cipher* dengan nilai pergeseran sesuai dengan nilai karakter pada kunci. Hasil pembentukan kunci tersebut akan digunakan untuk membentuk kunci baru menggunakan *vigenere cipher*. Sehingga kunci baru akan digunakan untuk menyandikan data teks dengan memanfaatkan algoritma *vigenere cipher*. Bahasa pemrograman yang digunakan pada penelitian ini adalah java.

III. ALGORITMA

Pembentukan algoritma baru dalam penerapan *vigenere cipher* dimulai dengan mengolah pesan (P) dan kunci (K) yang dimasukkan oleh pengguna. Semua karakter pada pesan dan kunci akan dirubah menjadi huruf kapital. Pengubahan dilakukan karena algoritma baru hanya akan mengolah karakter huruf kapital. Proses selanjutnya membentuk kunci yang digunakan untuk mengenkripsi pesan (P).

Pembentukan kunci tahap pertama dilakukan dengan menggunakan algoritma *caesar cipher*. Kunci masukan dari pengguna akan dienkripsi dengan nilai posisi karakter pesan yang berhubungan dengan karakter kunci. Sebagai contoh terdapat pesan "AKU ADA DISINI" dan kunci "KITA". Karakter "K" pada kunci akan berhubungan dengan "A" pada pesan. Nilai posisi karakter "A" pada pesan akan bernilai 1, sehingga karakter "K" yang akan dienkripsi dengan kunci akan bernilai 1. Karakter selanjutnya "K" pada pesan akan berhubungan dengan karakter "I" pada kunci. Nilai posisi karakter "K" adalah 2, sehingga karakter "I" yang akan dienkripsi dengan kunci bernilai 2. Algoritma ini akan berjalan begitu seterusnya sampai semua karakter pesan berhubungan dengan semua karakter kunci. Hasil dari tahap pertama akan disebut sebagai kunci pertama atau $K1$.

Tahap kedua pada pembentukan kunci dilakukan dengan menggunakan algoritma *vigenere cipher*. $K1$ digunakan sebagai bahan yang akan dienkripsi dan kunci dari masukan pengguna akan digunakan sebagai kunci enkripsi. Proses enkripsi ini tidak mengalami perubahan dalam hal algoritma. $K1$ akan dienkripsi dengan kunci K sesuai dengan algoritma enkripsi *vigenere cipher* yang telah ada. Hasil enkripsi pada tahap kedua adalah kunci terakhir atau *final key* (FK).

Tahap enkripsi terakhir adalah mengenkripsi pesan (P) menggunakan algoritma *vigenere cipher* dengan kunci FK. Penggunaan algortima *vigenere cipher* pada tahap ini juga tidak mengalami perubahan. Enkripsi pesan (P) dengan kunci FK akan sesuai dengan kaidah enkripsi algoritma *vigenere cipher* yang telah ada. Pesan yang ditampilkan pada pengguna sebagai hasil penerapan algoritma *vigenere cipher* dengan cara baru merupakan hasil enkripsi pada tahap ini.

IV. MODEL MATEMATIS

A. Caesar Cipher

Caesar cipher digunakan sebagai pembentuk kunci untuk digunakan pada proses enkripsi pesan. Algoritma *caesar cipher* akan menggeser nilai dari karakter pesan (P) sejauh kunci (K), dengan K merupakan nilai integer. Misal terdapat pesan "SIX" dan digeser sejauh K=3, maka *cipher text* tersebut adalah "VLA". Pada *caesar cipher* huruf A, B, C, ..., Z akan diberi label dengan angka 0, 1, 2, ..., 25 [4]. Model matematis untuk *caesar cipher* dapat dihitung dengan menggunakan persamaan (1) :

$$C = E(P, K) = (P + K) mod\ 26 \quad (1)$$

Keterangan :

C = *Cipher Text*

$E(P, K)$ = Enkripsi P dengan kunci K

P = Pesan

K = Kunci pergeseran

Pada penelitian ini menggunakan modifikasi algoritma *vigenere cipher* sehingga algoritma *caesar cipher* akan mengalami perubahan. Perubahan dilakukan dengan menggunakan nilai posisi pesan (i) sebagai kuncinya. Persamaan (2) merupakan modifikasi persamaan dari persamaan (1) sebagai berikut :

$$C = E(P_i, i) = (P_i + i) mod\ 26 \quad (2)$$

Keterangan :

C = *Cipher Text*

$E(P_i, i)$ = Enkripsi P_i dengan kunci i

P_i = Karakter pesan ke i

i = Kunci pergeseran

B. Vigenere Cipher

Vigenere cipher merupakan *polyalphabetic substitution cipher* dan dikembangkan dari modifikasi *caesar cipher*. *Vigenere cipher* dianggap sebagai sistem enkripsi yang paling aman dibandingkan dengan *polyalphabetic substitution cipher* lain [3]. Pada *vigenere cipher*, kunci yang digunakan berupa karakter yang dimasukan oleh pengguna. Sebagai contoh terdapat kunci "ENCODE" dan pesan "THE SKY IS FALLING". Proses enkripsi dimulai dengan menyesuaikan setiap huruf dengan angka 0 sampai 25 (A=0, B=1, C=2, ..., Z=25). Hasil enkripsi didapatkan dari menambahkan nilai pesan dengan kunci. Hasil akan dikurangi 26 apabila nilai hasil lebih dari 25. *Cipher text* dari enkripsi adalah XUGGNCMFHOOPMAI. Model matematis algoritma enkripsi *vigenere cipher* dapat dihitung dengan menggunakan persamaan (3) :

$$E(x) = (x + n)\ mod\ 26 \quad (3)$$

Keterangan :

$E(x)$ = Enkripsi karakter x

x = karakter pada pesan

n = karakter pada kunci

Sedangkan algoritma dekripsi *vigenere cipher* dapat diketahui dengan menggunakan persamaan (4) :

$$D(c) = (c - n)\ mod\ 26 \quad (4)$$

Keterangan :

$D(c)$ = Dekripsi karakter c

x = karakter pada pesan

n = karakter pada kunci

c = karakter pada *cipher text*

C. Modifikasi algoritma vigenere cipher

Penelitian ini akan menggunakan algoritma gabungan antara *caesar cipher* dan *vigenere cipher*. Jika kunci pertama dibentuk menggunakan algoritma *caesar cipher* dengan kunci (K) sebagai masukan maka hasil enkripsi disebut sebagai kunci pertama ($K1$). Persamaan (5) menunjukkan model matematis $K1$:

$$K1 = (K_j + i) mod\ 26 \quad (5)$$

Keterangan :

$K1$ = Kunci pertama

K_j = Karakter kunci ke j

i = Nilai posisi pesan yang berhubungan K_j

$K1$ akan digunakan untuk membentuk *final key (FK)* dengan menggunakan algoritma *vigenere cipher*. Persamaan pembentukan FK dapat dilihat pada persamaan (6) :

$$FK = (K1 + K) mod\ 26 \quad (6)$$

Keterangan :

FK = *final key*

$K1$ = kunci pertama

K = kunci masukan dari pengguna

Hasil enkripsi pesan didapatkan dari menyandikan pesan dengan *final key* menggunakan *vigenere cipher* yang terlihat pada persamaan (7).

$$C = (P + FK) mod\ 26 \quad (7)$$

Keterangan:

C = *Cipher text*

P = Pesan

FK = *Final key*

V. HASIL PENELITIAN DAN PEMBAHASAN

Pesan yang digunakan adalah "IN THE FOREST THERE ARE MANY TREES WITH THE SAME HEIGHT FOR EXAMPLE MANY" dengan kunci pesan "ZHW"

A. Hasil dari Vigenere Cipher

Pesan : IN THE FOREST THERE ARE MANY TREES WITH THE SAME HEIGHT FOR EXAMPLE MANY

Kunci : SIGU

Final Key : SIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSI

Cipher text: AV ZBW NULWAZ NZMXY SZK GSVE NJMKM OQZB LPK MSUK BWQMBL NUL WFGGHTK GSVE

Gambar 1. Hasil simulasi *vigenere cipher* dengan menggunakan 4 karakter pada kunci.

Gambar 1. menunjukkan bahwa hasil simulasi *vigenere cipher* terdapat pengulangan kata pada *cipher text*. Hal ini dikarenakan informasi pesan di enkripsi dengan kata yang berulang pada *final key*. Dengan adanya pengulangan kata dalam *final key* sehingga mengakibatkan adanya peluang informasi pesan dapat diprediksi. Pada penelitian ini prediksi informasi pesan dapat menggunakan metode *kasiski* [4]. Oleh karena itu metode *vigenere cipher* memiliki peluang pencurian data berupa teks.

B. Hasil dari Modifikasi Algoritma Vigenere Cipher

Pesan : IN THE FOREST THERE ARE MANY TREES WITH THE SAME HEIGHT FOR EXAMPLE MANY

Kunci : SIGU

Final Key : LSPSPWTWTAXAXEBEBIFIFMJMJQNQNURURYVYVCZCZGDGDKHKHOLOLSLSPSPWTWTAXAXEBEBIFIFMJMJQNQNURURYVYVCZCZGDGDKHKHOLOLS

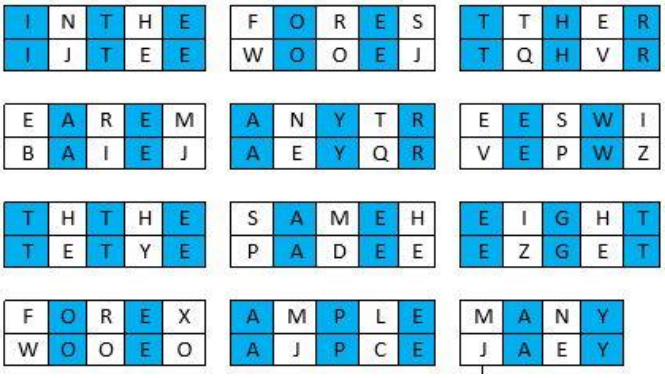
Cipher text : TF IZT BHNXSQ TEISI BZJ UFZH FAURI JCKB KFZ QVOD JDOJNW PVB LLLAADT EPJR

Gambar 2. Hasil simulasi modifikasi *vigenere cipher* dengan menggunakan 4 karakter pada kunci.

Hal yang berbeda terlihat pada Gambar 2. dimana hasil simulasi modifikasi *vigenere cipher* tidak ada pengulangan kata pada *cipher text*. Hal ini dikarenakan informasi pesan di enkripsi dengan kata yang tidak berulang pada *final key* sehingga informasi pesan tidak dapat diprediksi. Oleh karena itu disarankan agar metode modifikasi *vigenere cipher* digunakan dalam enkripsi infotmasi data berupa teks.

C. Nilai peluang prediksi informasi pesan

Gambar 3. menunjukkan bahwa perbandingan hasil prediksi informasi pesan memiliki beberapa informasi yang sama dengan aslinya. Pada baris pertama dalam Gambar 3. merupakan informasi asli dengan menggunakan enkripsi *vigenere cipher*. Sedangkan baris kedua merupakan prediksi informasi pesan dengan menggunakan kasiski [4].



Gambar 3. Contoh hasil prediksi informasi pesan dengan menggunakan metode kasiski [4].

Berdasarkan Gambar 3. maka dapat diketahui bahwa nilai peluang informasi pesan diketahui sebesar 55,56%. Hal ini menunjukkan bahwa metode *vigenere cipher* memiliki peluang dalam pencurian informasi data.

		Peluang	
		Vigenere Cipher	Modifikasi *Vigenere Cipher*
Jumlah Karakter Kunci	3 Karakter	74,07%	0,00%
	4 Karakter	55,56%	0,00%
	5 Karakter	27,78%	0,00%
	6 Karakter	55,56%	0,00%

Gambar 4. Perbandingan nilai peluang prediksi informasi pesan antara *vigenere cipher* dan modifikasi *vigenere cipher*.

Gambar 4. menunjukkan bahwa perbandingan nilai peluang prediksi informasi pesan antara *vigenere cipher* dan modifikasi *vigenere cipher* sangat besar. Peluang terbesar informasi metode *vigenere cipher* adalah 74,07 % pada 3 karakter kunci. Hal ini menunjukkan bahwa informasi pesan dengan metode *vigenere cipher* memiliki tingkat keamanan yang rendah. Hal ini dikarenakan semakin tinggi nilai peluang prediksi informasi pesan maka semakin mudah informasi pesan di prediksi. Sedangkan informasi pesan yang dienkripsi dengan menggunakan modifikasi *vigenere cipher* memiliki nilai peluang 0% sesuai dengan Gambar 4. Hal ini dikarenakan hasil enkripsi pada modifikasi *vigenere cipher* tidak memiliki pola perulangan kata. Hal ini menujukkan bahwa meotde modifikasi *vigenere cipher* memiliki tingkat keamanan data yang lebih baik daripada metode *vigenere cipher*. Oleh karena itu disarankan metode modifikasi *vigenere cipher* dapat digunakan dalam prosedur keamanan data.

VI. KESIMPULAN

Hasil simulasi menunjukkan metode *vigenere cipher* memiliki pengulangan kata pada *final key* sehingga memiliki peluang informasi pesan dapat diprediksi. Sedangkan metode modifikasi *vigenere cipher* tidak memiliki pengulangan kata pada *final key* sehingga informasi pesan tidak dapat diprediksi. Pada metode *vigenere cipher* memiliki nilai peluang terbesar informasi dapat diprediksi sebesar 74,07 %. Kelebihan algoritma modifikasi *vigenere cipher* adalah hasil enkripsi tidak memiliki pola perulangan huruf atau kata.

DAFTAR PUSTAKA

[1] Nishika dan R.K. Yadav, "A Lookup Table Based Secure Cryptographic SMS Communication on Android Environment". International Journal of Computer Science and Mobile Computing Vol. 2(6), pp. 53-59.

[2] Narender T. Dan Anita G.,"Comparative Analysis of Symmetric Key Encryption Algorithms". International Journal of Advanced Research in Computer Science and Software Engineering Vol. 4(8), pp. 348-354.

[3] David Solomon, "Data Privacy and Security". Springer, 2003.

[4] A. A. Bruen dan M. A. Forcinito, "Cryptography, Information Theory, and Error-Correction : A Handbook for The 21st Century", New Jersey: John Wiley & Sons Inc., 2005.

[5] Q. A. Kester, "A Cryptosystem Based on Vigenere Cipher with Varying Key". International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Vol.1(10), pp.108-113.