METODA *VIGENERE CHIPER DOUBLE COLUMNAR TRANSPOSITION* SEBAGAI MODIFIKASI TEKNIK KRIPTOGRAFI DALAM PEMBENTUKAN KUNCI

Hendro Eko Prabowo[1], **Arimaz Hangga**[1]
[1] Jurusan Teknik Elektro, Fakultas Teknik, Universitas Negeri Semarang
Kampus UNNES, Kel. Sekaran, Kec. Gunung Pati, Semarang, Jawa Tengah 50229.
[*]Email: hendro.prabowo15@gmail.com

Abstrak

Tindakan pencurian data sering terjadi pada pertukaran informasi yang menggunakan jaringan komunikasi. Teknik kriptografi merupakan salah satu alternatif untuk meminimalkan tindakan pencurian data khususnya data berupa teks dengan memberikan prosedur keamanan. Salah satu metoda kriptografi yang dapat digunakan dalam memberikan prosedur keamanan adalah metoda vigenere cipher double columnar transposition. Metoda tersebut telah terbukti mampu memberikan modifikasi pembentukan kunci data teks sehingga dapat meningkatkan prosedur keamanan tersebut. Hasil enkripsi dari modifikasi vigenere cipher juga tidak memiliki perulangan kata yang merupakan kekurangan dari vigenere cipher.

***Kata kunci**: data teks, kriptografi, vigenere cipher*

1. PENDAHULUAN

Teknik keamanan data terus dikembangkan untuk meminimalkan pencurian data. Peningkataan prosedur kemanan data sering dikembangkan agar data tidak dapat dicuri. Penyandian atau enkripsi data merupakan proses pengubahan informasi data agar data tidak dapat terbaca oleh pihak yang tidak berkepentingan. Hasil dari enkripsi adalah informasi yang disandikan atau *cipher text*. Sedangkan proses pengambilan informasi dari sandi disebut dekripsi (Nishika dan Yadav, 2013). Algoritma kriptografi digunakan pada proses enkripsi maupun dekripsi. Pada umumnya algoritma kriptografi dibedakan menjadi dua jenis, yaitu kriptografi kunci simetris *(symmetric key cryptography)* dan kriptografi kunci tidak simetris *(asymmetric key cryptography)*(Tyagi dan Anita, 2014).

Kriptografi kunci simteris merupakan algoritma kriptografi yang menggunakan kunci yang sama dalam proses enkripsi dan dekripsi. Sedangkan pada kriptografi kunci tidak simetris merupakan algoritma yang menggunakan kunci berbeda. Pada proses enkripsi menggunakan *public key* dan proses dekripsi menggunakan *private key*. *Private key* hanya diketahui oleh pendekripsi *cipher text*.

Vigenere cipher adalah salah satu contoh metode kriptografi kunci simeteris dengan tingkat keamanan kunci yang lebih sulit dipecahkan. Hal ini disebabkan algoritma dari *vigenere cipher* menggunakan kunci enkripsi berupa huruf dan berbentuk polialfabetik(Solomon, 2003). 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*.

2. METODE PENELITIAN

Pada penelitian ini menggunakan *vigenere cipher*, *caesar cipher*, dan *columnar transposition cipher*. *Caesar cipher* dan *double columnar transposition cipher* digunakan untuk pembentukan kunci yang akan digunakan pada enkripsi metode *vigenere cipher*. Kunci masukan dari pengguna akan dienkripsi menggunakan *caesar cipher* dengan nilai posisi karakter sebagai kunci enkripsi. Hasil pembentukan kunci tersebut digunakan untuk membentuk kunci baru menggunakan *vigenere cipher*. Kunci akhir *(final key)* didapatkan dengan menyandikan pembentukan kunci baru dari *vigenere cipher* dengan memanfaatkan metode *double columnar transposition cipher*. Sehingga penyandian informasi dari pengguna menggunakan metode *vigenere cipher* dengan *final key* sebagai kunci enkripsi.

3. ALGORITMA

Pembentukan algoritma baru dalam penerapan *vigenere cipher* dimulai dengan mengolah pesan (P) dan kunci (K) masukan dari pengguna. Karakter pada pesan dan kunci dirubah menjadi

huruf kapital. Pengubahan dilakukan karena algoritma *vigenere cipher* 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 pengguna akan dienkripsi menggunakan nilai posisi karakter pesan sebagai kunci, contoh terdapat pesan "KAMI ADALAH SATU" dan kunci "DIA". Karakter "D" pada kunci akan berhubungan dengan "K" pada pesan. Nilai posisi karakter "K" adalah 1, maka karakter "D" pada kunci akan dienkripsi dengan kunci enkripsi bernilai 1. Karakter selanjutnya "I" berhubungan dengan karakter "A" pada pesan dengan nilai posisi 2, sehingga karakter "I" akan dienkripsi dengan kunci 2. Algoritma ini akan berjalan begitu seterusnya sampai semua karakter pesan memiliki satu pasang karakter pada kunci. Hasil dari tahap pertama adalah kunci pertama atau $K1$.

Tahap kedua pembentukan kunci dilakukan dengan memanfaatkan algoritma *vigenere cipher*. $K1$ digunakan sebagai pesan yang akan dienkripsi untuk pembentukan kunci kedua dengan kunci masukan pengguna (K) sebagai kunci enkripsi. Algoritma proses enkripsi pada tahap ini tidak mengalami perubahan. $K1$ akan dienkripsi dengan kunci K sesuai dengan enkripsi *vigenere cipher* yang telah ada. Hasil dari enkripsi tahap kedua adalah kunci kedua atau $K2$.

Tahap ketiga adalah membentuk kunci akhir yang didapatkan dari penyandian $K2$ dengan kunci K sebagai kunci enkripsi menggunakan algoritma *double columnar transposition cipher*. Tahap pembentukan ini memiliki dua proses, yaitu proses pertama menggunakan kunci K sedangkan proses kedua menggunakan kunci K yang dibalik posisi karakternya sebagai kunci enkripsi. Proses pertama $K2$ digunakan sebagai informasi yang akan dienkripsi menggunakan kunci K dengan hasil K3. Proses kedua menggunakan K3 sebagai infomasi yang akan dienkripsi menggunakan kunci K yang dibalik sehingga menghasilkan kunci akhir atau *final key* (FK).

Tahap terakhir adalah menyandikan pesan (P) menggunakan algoritma *vigenere cipher* dengan kunci FK. Penggunaan algoritma *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. Hasil enkripsi atau *cipher text* yang ditampilkan adalah hasil dari penerapan algoritma *vigenere cipher* dengan cara baru.

4. MODEL MATEMATIS

4.1 *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 (Bruen dan Foricinito, 2005). 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 :

ISBN 978-602-99334-4-4

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

Keterangan :

C = *Cipher Text*

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

P_i = Karakter pesan ke i

i = Kunci pergeseran

4.2 *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 (Solomon, 2005). 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 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*

4.3 *Double Columnar Transposition Cipher*

Double columnar transposition cipher merupakan algoritma enkripsi hasil pengembangan dari *columnar transposition cipher*. Pada *double columnar transposition cipher* algoritma enkripsi sesuai dengan *columnar tranpsition cipher* namun proses enkrpisi dilakukan dua kali. Kedua proses enkripsi tersebut dapat menggunakan kunci yang sama maupun kunci yang berbeda(Pramanik, 2014). Model matematis proses enkripsi *columnar transposition cipher* didefinisikan sebagai berikut(Kester, 2013) :

$$Ct\ of\ P = \begin{pmatrix} Y_0 & \ldots\ldots & Y_l \\ X_{po_1} & \ldots\ldots & X_{pl_1} \\ X_{po_2} & \ldots\ldots & X_{pl_2} \\ \vdots & & \vdots \\ X_{po_m} & \ldots\ldots & X_{pl_m} \end{pmatrix} \quad (5)$$

Keterangan :

$Ct\ of\ P$ = *Columnar Transposition* dari pesan

Y_0 = karakter pertama dari kunci

Y_l = karakter terakhir dari kunci

X_{po_1} = karakter pertama dari pesan yang berelasi dengan Y_0

X_{pl_1} = karakter pertama dari pesan yang berelasi dengan Y_l

X_{po_m} = karakter terakhir dari pesan yang berelasi dengan Y_0

X_{pl_m} = karakter terakhir dari pesan yang berelasi dengan Y_l

Apabila $Ct\ of\ P$ didefinisikan sebagai CtP_i dengan i adalah integer, maka hasil enkripsi dari algoritma *columnar transposition cipher* dimodelkan sebagai :

$$Cp = \{C_tP_1 + C_tP_2 + C_tP_3 + \cdots + C_tP_m\} \quad (6)$$

Keterangan :

Cp = Hasil enkripsi *(cipher text)*

m = Kolom terakhir pada persamaan (5)

4.4 *Modifikasi algoritma vigenere cipher*

Penelitian ini akan menggunakan algoritma gabungan antara *caesar cipher*, *vigenere cipher* dan *doubel columnar transposition cipher*. Jika kunci pertama dibentuk menggunakan algoritma *caesar cipher* dengan kunci (K) sebagai masukan maka hasil enkripsi disebut sebagai kunci pertama ($K1$). Persamaan (7) menunjukkan model matematis $K1$:

$$K1 = (K_j + i) mod\ 26 \quad (7)$$

Keterangan :

$K1$ = Kunci pertama

K_j = Karakter kunci ke j

i = Nilai posisi pesan yang berhubungan K_j

$K1$ akan digunakan untuk membentuk kunci kedua ($K2$) dengan menggunakan algoritma *vigenere cipher*. Persamaan pembentukan $K2$ dapat dilihat pada persamaan (8) :

$$K2 = (K1 + K) mod\ 26 \quad (8)$$

Keterangan :

$K2$ = kunci kedua

ISBN 978-602-99334-4-4

$K1$ = kunci pertama

K = kunci masukan dari pengguna

Pembentukan *final key* yang akan digunakan untuk proses enkripsi pesan didapatkan dari menyandikan $K2$ dengan kunci K menggunakan algoritma *double columnar transposition cipher*. Apabila pada persamaan (5) pesan yang digunakan adalah $K2$, maka dapat didefinisikan bahwa :

$$Ct\ of\ P = Ct\ of\ K2 = CtP_i \quad (9)$$

dengan hasil enkripsi sesuai dengan persamaan (6) adalah Cp yang merupakan *final key*. Hasil enkripsi pesan didapatkan dari menyandikan pesan dengan *final key* menggunakan *vigenere cipher* yang terlihat pada persamaan (10).

$$C = (P + FK) mod\ 26 \quad (10)$$

Keterangan:

C = *Cipher text*

P = Pesan

FK = *Final key*

5. HASIL PENELITIAN DAN PEMBAHASAN

Pesan yang digunakan adalah "IN THE FOREST THERE ARE MANY TREES WITH SAME HEIGHT FOR EXAMPLE MANY" dengam kunci pesan "SIGU".

5.1 Hasil dari *Vigenere Cipher*

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

Kunci : SIGU

Final Key : SIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSIGUSI

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 kunci.

Gambar 1 memperlihatkan kelemahan *vigenere cipher* dengan adanya rangkaian karakter berulang pada hasil enkripsi. Perulangan kata diakibatkan karena kunci yang digunakan pada proses enkripsi diulang hingga memenuhi panjang dari pesan yang akan disandikan. Adanya kejadian tersebut dapat dimanfaatkan untuk memecahkan sandi yang dibentuk dengan *vigenere cipher* (Bruen dan Forcinito, 2005). Sehingga dengan metode *vigenere cipher* yang telah ada memiliki peluang informasi data dapat dicuri.

5.2 Hasil dari Modifikasi Algoritma *Vigenere Cipher*

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

Kunci : SIGU

Final Key : TJZPEUKPFVLEUKXNDSIYOTJZSIYOBRHWMCSXNDWMCSPFV LAQGLBRHAQG

Cipher Text : BW SWI ZYGJNE XBOOR DJM KOGH SJMCG XZAD ECEB UHESJL UTM PXQSAMV TADE

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

Gambar 2 memperlihatkan hasil penyandian pesan dengan algoritma modifikasi *vigenere cipher*. Pada algoritma modifikasi *vigenere cipher*, kunci dibentuk ulang sehingga menghasilkan kunci baru untuk menyandikan pesan. Sandi yang dihasilkan juga tidak memiliki rangkaian karakter perulangan yang merupakan kelemahan dari sandi *vigenere cipher* yang telah ada. Oleh karena itu modifikasi *vigenere cipher* dapat mengurangi kelemahan dari algoritma *vigenere cipher* yang telah ada.

6. KESIMPULAN

Hasil simulasi menunjukkan metode *vigenere cipher* memiliki rangkaian perulangan kata pada hasil penyandian yang merupakan kelemahan algoritma tersebut. Karakter berulang yang dimaksud adalah NULW dan KGSVE. Hal ini dikarenakan, kunci yang digunakan untuk penyandian diulang sampai beberapa kata sesuai dengan panjang karakter pesan. Berbeda dengan algoritma modifikasi *vigenere cipher* yang tidak memiliki rangkaian perulangan kata pada hasil penyandian. Kejadian tersesebut dikarenakan kunci pada modifikasi algoritma *vigenere cipher* dibentuk ulang untuk meminimalkan perulangan pada kata. Oleh karena itu modifikasi *vigenere cipher* dapat digunakan untuk memperbaiki algoritma *vigenere cipher* yang telah ada.

7. DAFTAR PUSTAKA

Bruen, A.A., and M. A. Forcinito, (2005), *Cryptography, Information Theory, and Error-Correction: A Handbook of 21st Century*, John Wiley & Sons Inc., New Jersey.

Kester, Q.A., (2013), A Hybird Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher, *International Journal od Advanced Technology and Engineering Research (IJATER) Vol. 3(1)*, pp. 141-147.

Nishika and R.K. Yadav, (2013), 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.

Pramanik, M.B., (2014), Implementation of Cryptography Technique Using Columnar Transposition, *International Journal of Computer Applications*, pp. 19-23.

Solomon, D., (2003), *Data Privacy and Security*, Springer-Verlag New York Inc., New York.

Tyagi, N., and Anita G., (2014), Comparative Analysis of Symmetric Key Encryption Algorithms, *International Journal of Advanced Research in Computer Science and Software Engineering Vol.4(8)*, pp. 348-354.

ISBN 978-602-99334-4-4