PENGAMANAN FILE TEKS MENGGUNAKAN KOMBINASI ALGORITMA *VIGINERE CIPHER* DAN *TRIPLE COLUMNER*

Miske Silangen, Stendy Sakur, Desmin Tuwohingide
Jurusan Teknik Komputer dan Komunikasi, Politeknik Negeri Nusa Utara
Jln.Kesehatan no.1, Kelurahan Sawang Bendar, Kecamatan Tahuna Kabupaten Kepulauan Sangihe
miske.silangen@yahoo.com

Abstrak: Data yang bersifat rahasia perlu dijaga keamanannya. Pada umumnya metode yang digunakan untuk pengamanan data adalah dengan membuat pasword yang terdiri dari beberapa karakter sehingga sering terjadi keboboloan karena pasword yang digunakan mampu ditebak dengan cepat. Meningkatkan keamanan pesan bisa dilakukan dengan teknik kriptografi. Pada teknik ini pesan akan dienkripsi (disandikan) menggunakan metode tertentu sehingga pesan tersebut sulit untuk dibaca karena susunan hurufnya tidak mengandung makna.
Pada penelitian ini digunakan Metode vigenere cipher untuk menyandikan kunci yang akan digunakan untuk melakukan enkripsi. pada metode Vigenere cipher tiap karakter ke-i pada teks asli ditambah dengan kunci indeks ke-i vigenere, kemudian di-mod p dimana p adalah panjang kunci vigenere. Sedangkan metode triple columner digunakan untuk menyandikan plaintext atau pesan asli. Pada metode ini pesan dienkripsi sebanyak tiga kali sehingga lebih meningkatkan keamanan pesan. Setelah dilakukan pengujian, kedua metode tersebut bisa digunakan untuk menyandikan pesan dan mengembalikan pesan tersebut ke bentuk semula, sehingga aplikasi yang dibuat diharapkan bisa digunakan untuk mengirim pesan yang bersifat rahasia. Hal ini perlu dilakukan untuk menghindari kehilangan data sehingga pesan yang dikirim bisa diterima oleh penerima pesan tanpa mengalami perubahan data.

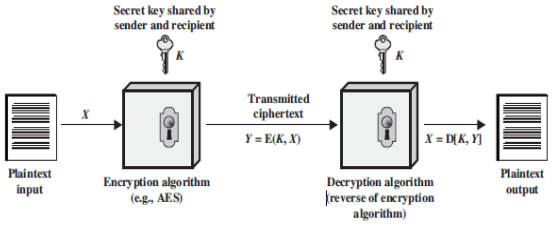
Kata kunci: *Kriptografi, Enkripsi, Dekripsi, Viginere, Triple Columner.*

1. PENDAHULUAN

Data yang bersifat rahasia perlu dijaga keamanannya. Pada umumnya metode yang digunakan untuk pengamanan data adalah dengan membuat pasword yang terdiri dari beberapa karakter sehingga sering terjadi kebobolan karena pasword yang digunakan mampu dengan cepat ditebak. Kemajuan teknologi saat ini memungkinkan kita untuk bertukar informasi menggunakan media digital melalui jaringan internet. Namun bertukar informasi dengan cara ini meningkatkan resiko penyadapan terhadap informasi penting (Silangen, 2017).

Meningkatkan keamanan pesan bisa dilakukan dengan teknik kriptografi. Pada teknik ini pesan akan dienkripsi (disandikan) menggunakan metode tertentu sehingga pesan tersebut sulit untuk dibaca karena susunan hurufnya tidak mengandung makna. Untuk bisa membaca pesan tersandi maka harus dilakukan dekripsi yaitu proses untuk mengembalikan pesan tersandi menjadi bentuk pesan yang bisa dibaca.

Dalam proses enkripsi maupun dekripsi diperlukan kunci. Kunci pada kriptografi terdiri dari dua jenis yaitu kunci simetri dan kunci asimetri. Kunci simetri adalah kunci yang sama artinya kunci yang digunakan untuk melakukan enkripsi maupun dekripsi adalah kunci yang sama biasanya disebut kunci *private*. Sedangkan kunci asimetri merupakan kunci yang berbeda baik dalam melakukan enkripsi maupun dekripsi disebut kunci publik. Skemanya diperlihatkan pada Gambar 1.



Gambar 1. kunci simetri (Stalling, 2011)

Dalam mengamankan data dan informasi ada syarat yang harus dipenuhi yaitu kerahasiaan dan keutuhan data. Kerahasiaan ini mengandung makna menjaga kerahasiaan data yang dikirim ke penerima agar tidak diketahui

oleh pihak lain dan untuk membatasi akses dari orang-orang yang berusaha mengetahui isi pesan ataupun merusak pesan tersebut. Sedangkan keutuhan data yaitu menjaga data tersebut agar benar-benar utuh dan bisa sampai ke penerima tanpa dimodifikasi oleh pihak-pihak yang tidak berhak atas informasi tersebut, tanpa mendapatkan ijin dari pemilik informasi (Stalling, 2011).

Penelitian tentang kriptografi pernah dilakukan oleh Pardede, (2014) menggunakan kriptografi metode *Columner* atau transposisi kolom dengan satu kunci. Hasil penelitian tersebut metode *columner* dengan satu kunci bisa digunakan untuk mengamankan data.

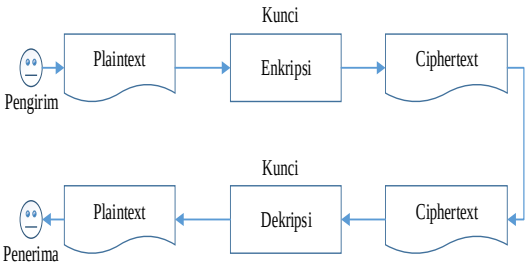
Penelitian yang akan diusulkan adalah lebih meningkatkan sistem keamanan dengan menggunakan dua metode yaitu metode *vigenere* dan metode *triple columner*. metode *vigenere* digunakan untuk menyandikan kunci, sedangkan metode *triple columner* digunakan untuk menyandikan pesan.

Dalam melakukan enkripsi pada metode *Vigenere cipher* tiap karakter ke-i pada teks asli ditambah dengan kunci indeks ke-i vigenere, kemudian di-mod *p* dimana *p* adalah panjang kunci vigenere. Sedangkan pada proses dekripsi tiap karakter ke-i pada teks sandi dikurang dengan kunci indeks ke-i mod *p* (Sadikin, 2012).

Dalam melakukan enkripsi pada metode *triple columner* yaitu dengan menulis karakter teks asli dengan orientasi baris dengan panjang karakter yang sama. Kemudian menulisnya kembali namun degan orientasi kolom sehingga melalui proses tersebut akan didaptkan pesan tersandi. Pada proses dekripsi jumlah baris dapat dihitung dengan membagi panjang teks sandi dengan panjang kunci selanjutnya mengisi kolom terlebih dahulu sesuai dengan urutan kunci yang telah disepakati bersama, dengan teks sandi sampai baris terakhir.(Sadikin, 2012).

2. METODE PENELITIAN

Terdapat dua proses yang dilakukan pada penelitian kriptografi yaitu proses enkripsi dan dekripsi. Enkripsi merupakan proses untuk menyandikan pesan. Hasil penyandian pesan disebut *ciphertext*, sedangkan dekripsi merupakan proses untuk mengembalikan *ciphertext* menjadi pesan asli atau *plaintext*. Dalam melakukan enkripsi maupun dekripsi dibutuhkan kunci. Pada penelitian ini digunakan kunci simetris dimana pengirim dan penerima pesan menggunakan kunci yang sama. Pengirim pesan melakukan proses enkripsi sedangkan penerima pesan melakukan proses dekripsi. Bahasa Pemrograman yang digunakan adalah Qt/C++ Frame Work. Untuk huruf yang digunakan pada penelitian adalah huruf kapital. Skema proses enkripsi dan dekripsi secara umum diperlihatkan pada Gambar 2.



Gambar 2. Skema umum enkripsi dan dekripsi

3. KRIPTOGRAFI

Kriptografi adalah algoritma yang sangat baik digunakan untuk mengamankan pesan rahasia baik pesan dalam bentuk teks, audio, maupun video. Pengertian yang lain Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Sehingga dengan adanya teknik-teknik tertentu pada kriptografi maka pesan rahasia yang dikirimkan ke penerima pesan bisa terjaga keamanannya (Menezes, 1997).

3.1 *Vigenere Cipher*

Vigenere chiper merupakan sistem sandi poli-alfabetik. Pada metode *vigenere cipher* kunci yang digunakan adalah karakter. Dalam melakukan enkripsi pada metode *Vigenere cipher* tiap karakter ke-i pada teks asli ditambah dengan kunci indeks ke-i vigenere, kemudian di-mod *p* dimana *p* adalah panjang kunci *vigenere*. Sedangkan pada proses dekripsi tiap karakter ke-i pada teks sandi dikurang dengan kunci indeks ke-i mod *p* (Sadikin, 2012).

Kunci yang digunakan pada *metode vigenere* harus sama panjang dengan *plaintext*, jika kunci yang digunakan pendek, maka akan diulang secara periodik. Contoh kunci yang digunakan misalnya AKU berjumlah 3 karakter sedangkan pesan asli adalah TERIMAKASIH berjumlah 11 karakter, maka kunci AKU akan diulang sampai memenuhi atau sama dengan panjang *plaintext*. Setiap pesan dengan alfabet dari A sampai Z, disesuaikan posisinya sehingga posisi A = 0, B = 1, C = 3, … ,Z = 25.

40 ***JURNAL BEHONGANG,*** *Volume 1, Nomor 2, hlm. 38-41*

Contoh penggunaan kunci secara periodik diperlihatkan pada Gambar 1.

Pesan	T	E	R	I	M	A	K	A	S	I	H
Kunci	A	K	U	A	K	U	A	K	U	A	K

Gambar 3 Contoh kunci periodik

3.2 *Triple Columner*

Columner merupakan jenis sandi transposisi. Cara kerja sandi *columner* adalah menulis karakter teks asli dengan orientasi baris dengan panjang karakter yang sama kemudian teks sandi didapatkan dengan menulis ulang dengan orientasi kolom. (Sadikin, 2012). Metode *Triple Columner* menggunakan 3 (tiga) jenis kunci yang digunakan pada proses enkripsi dan dekripsi.

4. HASIL DAN PEMBAHASAN

4.1 Hasil

Hasil dari penelitian ini adalah adanya apalikasi yang bisa digunakan sebagai pengamaan pada pesan teks yang bersifat rahasia yang dikirimkan ke penerima pesan, terlebih ketika pesan tersebut dikirimkan menggunakan jaringan internet. Proses enkripsi atau penyandian pesan serta proses dekripsi bisa dilakukan dengan baik. Pada penelitian ini kunci dan pesan teks dienkripsi terlebih dahulu, dimana kunci dienkripsi menggunakan metode *vigenere* sedangkan pesan teks dienkripsi menggunakan metode *triple columner. Dengan adanya kombinasi dua metode tersebut maka pesan rahasia bisa dikirimkan dengan aman* mengalami perubahan data oleh pihak-pihak yang tidak bertanggung jawab.

4.2 Pembahasan

4.2.1 Proses enkripsi metode Vigenere

Misalkan terdapat pesan KPK Kunci 5 6 8. Maka yang dilakukan adalah menyesuaikan pesan rahasia sesuai dengan posisi pengurutan alfabet dari angka 0-25. Kunci digunakan secara berurutan pada setiap satu huruf pesan kemudian dimodulo 26. Pesan pada huruf pertama yaitu K = 10 akan dienkripsi menggunakan kunci 5. Pesan berikutnya adalah P =15 dienkripsi menggunakan kunci 6, dan K dienkripsi menggunakan kunci 8. Prosesnya adalah:

10 + 5 mod 26 = 15 (P) ,
15 + 6 mod 26 = 21 (V),
10 + 8 mod 26 = 18 (S).

Hasil enkripsi dari pesan KPK dengan kunci 568 adalah PVS.

4.2.2 Proses dekripsi metode *Vigenere*

Dekripsi merupakan proses untuk mengembalikan pesan tersandi menjadi pesan yang bisa dibaca. Proses melakukan dekripsi yaitu karakter ke-i pada teks dikurang dengan kunci indeks ke-i mod *p* dimana *p* adalah panjang kunci *vigenere* . Contoh yang telah diuraikan sebelumnya bahwa pesan KPK dienkripsi menggunakan kunci 5 6 8 hasilnya adalah *ciphertext* PVS. Selanjutnya petahkan *ciphertext* tersebut sesuai dengan urutan alfabeth dari 0 sampai 25. Kunci digunakan secara berurutan pada setiap pesan.

Ciphertext dari pesan KPK adalah PVS. P = 15, V = 21, S = 18. Dilakukan dekripsi dengan kunci 5 6 8. Proses dekripsi adalah

15 -5 mod 26 = 10 (K)
21 - 6 mod 26 =15 (P)
18 - 8 mod 26 = 10 (K)

Sehingga ciphertext PVS bisa didekripsi sesuai dengan pesan asil yang dikirimkan yaitu KPK.

4.2.3 Triple Columner

Contoh proses enkripsi menggunakan metode *triple columner* dengan pesan TUNGGU SAYA DI PINTU SEBELAH TIMUR, dan kunci 1 yang digunakan yaitu 3 5 7 2 6 1 4.

kunci 2 adalah 7165342
kunci 3 adalah 4613257

Proses Enkripsi dengan metode *triple columner*:

Pesan = TUNGGU SAYA DI PINTU
SEBELAH TIMUR
Kunci = 3 5 7 2 6 1 4

Proses enkripsi tahap 1 menggunakan Kunci 1 = 7165342 diperlihatkan pada Tabel 1.

Tabel 1 Enkripsi menggunakan kunci 1

3	**5**	**7**	**2**	**6**	**1**	**4**
T	U	N	G	G	U	S
A	Y	A	D	I	P	I
N	T	U	S	E	B	E
L	A	H	T	I	M	U
R	H	I	J	K	L	M

*Ciphertext*1 yang didapatkan adalah UPBMLGDSTJTANLRSIEUMUYTAHGIEIKNAUHI

Proses enkripsi tahap 2 menggunakan Kunci 2 = 7165342.

Tabel 2. Enkripsi menggunakan kunci 2

7	**1**	**6**	**5**	**3**	**4**	**2**
U	P	B	M	L	G	D
S	T	J	T	A	N	L
R	S	I	E	U	M	U
Y	T	A	H	G	I	E
I	K	N	A	U	H	I

Ciphertext2 yang didapatkan adalah PTSTKDLUEILAUGUGNMIHMTEHABJIA NUSRYI

Proses enkripsi tahap 3 menggunakan Kunci 3 = 4613257

Tabel 3. Enkripsi menggunakan kunci 3

4	6	1	3	2	5	7
P	T	S	T	K	D	L
U	E	I	L	A	U	G
U	G	N	M	I	H	M
T	E	H	A	B	J	I
A	N	U	S	R	Y	I

Ciphertext3 yang didapatkan adalah SINHUKAIBRTLMASPUUTADUHJYTEGE NLGMII.

4.2.4 Dekripsi *triple columner*

Tahapan proses dekripsi dengan metode *triple columner*

*Ciphertext*3 merupakan hasil penyandian pesan pada tahap akhir. Untuk melakukan proses dekripsi, maka dimulai dengan melakukan dekripsi *ciphertext*3, menggunakan kunci 3 yaitu = SINHUKAIBRTLMASPUUTADUHJYTEGE NLGMII.

Kunci 3 = 4613257

Proses dekripsi tahap 1 menggunakan Kunci 3 = 4613257

Tabel 4 Dekripsi menggunakan kunci 3

4	6	1	3	2	5	7
P	T	S	T	K	D	L
U	E	I	L	A	U	G
U	G	N	M	I	H	M
T	E	H	A	B	J	I
A	N	U	S	R	Y	I

Hasil dekripsi pertama adalah *ciphertext* 3 yaitu PTSTKDLUEILAUGUGNMIHMTEHABJIA NUSRYI. Selanjutnya *ciphertext* 3 di-dekripsi menggunakan kunci 2.

Proses dekripsi tahap 2 menggunakan Kunci 2 = 7165342.

Tabel 5 Dekripsi menggunakan kunci 2

7	1	6	5	3	4	2
U	P	B	M	L	G	D
S	T	J	T	A	N	L
R	S	I	E	U	M	U
Y	T	A	H	G	I	E
I	K	N	A	U	H	I

Hasil dekripsi kedua adalah *ciphertext* 2 yaitu: UPBMLGDSTJTANLRSIEUMUYTAHGIEIK NAUHI. Selanjutnya dekripsi tahap akhir merupakan proses untuk mendapatkan pesan asli (*plaintext*).

Proses dekripsi tahap 3 menggunakan Kunci 1 = 3 5 7 2 6 1 4.

Tabel 6 Dekripsi menggunakan kunci 1

3	5	7	2	6	1	4
T	U	N	G	G	U	S
A	Y	A	D	I	P	I
N	T	U	S	E	B	E
L	A	H	T	I	M	U
R	H	I	J	K	L	M

Pada dekripsi tahap 3 didapatkan kembali pesan asli (*plaintext*) yakni TUNGGU SAYA DI PINTU SEBELAH TIMUR.

5 KESIMPULAN

1. Metode *vigenere cipher* dan *triple columner* dapat menyandikan pesan dan mengembalikannya ke bentuk semula.
2. Aplikasi yang dibuat bisa digunakan untuk mengirim pesan yang bersifat rahasia dengan aman.

6 SARAN

Pada penelitian ini pesan yang bisa dienkripsi adalah pesan dengan format teks. diharapkan kedepannya bisa melakukan enkripsi dengan format lain. Pada penelitian ini huruf yang bisa dienkripsi hanya huruf kapital diharapkan kedepannya bisa melakukan enkripsi dengan huruf kecil.

REFERENSI

Sadikin, R, 2012, Kriptografi untuk keamanan jaringan, Andi, Yogyakarta.

Silangen, M, 2017, Enkripsi dan penyembunyian data dalam file audio menggunakan *Triple Des* dan *parity coding,* Tesis, Universitas Gadjah Mada, Yogyakarta.

Stalling, W., 2011, *Cryptography and Network Security Principles and Practice, Fifth Edition, Prentice Hall*, New York.

Pardede, A. M. H., Maulita, Y, 2014, *Perancangan perangkat lunak enkripsi dan dekripsi file dengan metode transposisi kolom*, Jurnal Kaputama, Binjai, Vol. 8 No.1, ISSN 1979-6641.