ISSN: 2548-9704

IMPLEMENTASI ALGORITMA MODIFIKASI TRANSPOSISI COLUMNAR DALAM MENGAMAKAN DATA TEKS

Ika Anggriani

STMIK Budi Darma Medan
Jl. Sisingamangaraja No. 338 Simpang Limun Medan
Email : ikaanggri75@gmail.com

ABSTRAK

Masalah keamanan merupakan aspek paling penting dalam dunia teknologi informasi, misalnya : keamanan dokumen. Masalah keamanan dan kerahasiaan dokumen merupakan hal yang sangat penting dalam suatu pekerjaan, organisasi maupun pribadi.Hal ini mengakibatkan peerlunya suatu sistem pengamanan data dalam sebuah dokumen digital sehingga menjamin keamanan dari dokumen digital tersebut, baik dalam bentuk teks, gambar, suara maupun video. Oleh karena itu dibutuhkan suatu sistem yang dapat membantu dalam menjaga keamanan maupun kerahasian suatu data. Kriptografi merupakan salah satu metode pengamanan data yang dapat digunakan untuk menjaga keamanan maupun kerahasiaan dari suatu data. Dari permasalahan ini penulis akan merancang proses cara pengaman data teks menggunakan modifikasi transposisi columnar dan proses enkripsi dan dekripsi algoritma modifikasi transposisi columnar, sehingga orang ya ng tidak berhak tidak dapat membaca informasi ataupun melihat isi dari dokumen yang ada didalamnya. Dengan menggunakan modifikasi tranposisi columnar kita dapat mengunci data atau dokumen ya ng bersifatsi rahasia dengan proses penyandian yaitu enkripsi dan dekripsi. Transposisi columnar merupakan teknik kriptografi asimetri yang menggunakan dua buah kunci berbeda dalam proses enkripsi dan dekripsi. Kedua kunci tersebut dikenal dengan private key, yang digunakan untuk enkripsi data dan public key, yang digunakan untuk dekripsi data.dan pada laporan ini diuraikan teknik dasar modifikasi tranposisi columnar dapat diimplementasikan menggunakan aplikasi bahasa pemrograman visual basic 2008.

Kata kunci : Kriptografi, Algoritma, Keamanan Data, Modifikasi Transposisi Columnar

ABSTRACT

Security issues are the most important aspect in the world of information technology, for example: document security. The issue of security and confidentiality of documents is very important in a work, organization or personal. This results in the need for a system for securing data in a digital document so as to ensure the security of these digital documents, both in the form of text, images, sound and video. Therefore we need a system that can help maintain the security and confidentiality of data. Cryptography is one method of securing data that can be used to maintain the security and confidentiality of data. From this problem the writer will design the process of text data security using modification of columnar transposition and encryption and decryption algorithm algorithm modification of columnar transposition, so that people who are not entitled cannot read the information or view the contents of the documents inside. By using columnar transposition modification we can lock the data or document that has the secret character with the encryption process, namely encryption and decryption. Columnar transposition is an asymmetric cryptographic technique that uses two different keys in the encryption and decryption process. These two keys are known as private keys, which are used for data encryption and public key, which are used for data decryption. And in this report, the basic techniques for modifying columnar transpositions can be implemented using the application of Visual Basic 2008 programming language.

Keywords: Cryptography, Algorithms, Data Security, Modification of Columnar Transposition

1. PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi digital serta internet ini dapat digunakan secara “negatif” seperti pencurian atau perusakan data pada dokumen digital. Hal ini mengakibatkan perlunya suatu sistem pengamanan data dalam sebuah dokumen digital sehingga menjamin

ISSN: 2548-9704

keamanan dari dokumen digital tersebut, baik dalam bentuk teks, gambar, suara maupun video.

Teks ataupun tulisan merupakan dokumen yang paling banyak di buat dibandingkan dengan dokumen gambar ataupun lainnya. Setiap harinya banyak banyak dokumen yang berupa teks atau tulisan yang dihasilkan. Seiring dengan pertumbuhan dari dokumen elektronik ini timbul setidaknya dua masalah yaitu, pertama dari banyak dokumen yag di hasilkan beberapa diantara nya merupakan dokumen yang sifatnya rahasia dan pribadi. Hal ini tidak mengkhawatirkan apabila dokumen itu digunakan hanya untuk keperluan pribadi saja (tanpa perlu orang lain untuk mengetahui) karena dapat memanfaatkan fungsi penyandian pada dokumen dan hanya diri kita yang mengetahui penyandian tersebut, akan tetapi hal yang perlu diperhatikan adalah ketika dokumen yang bersifat rahasia ini diperlukan atau digunakan oleh banyak pihak sehingga penyadian yang digunakan untuk mengamankan data yang lebih kompleks, misalnya dengan teknik kriptografi.

Modifikasi transposisi columnar merupakan salah satu teknik kriptografi yang populer dan sudah cukup lama digunakan orang – orang. Modifkasi transposisi columnar merupakan salah satu metode kriptografi dimana pesan ditulis berderetan dari suatu panjang yang ditetapkan, lalu di baca kembali kolom perkolom dengan urutan pembacaan berdasarkan suatu kata kunci. Dan untuk memperkuat lagi proses penyandian ini maka dilakukan penggunaan modifikasi columnar tranposisi menggunakan fungsi dalam melakukan proses enkripsi dan depenelitian. Fungsi di gunakan untuk memisahkan huruf – huruf yang berbeda pada posisi ganjil dan genap. Maka itu akan membuat para kriptanalis sulit untuk mengetahui sandi yang telah di buat.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah, maka yang menjadi perumusan masalah adalah:

1. Bagaimana proses enkripsi dan depenelitian algoritma modifikasi tranposisi columnar?
2. Bagaimana proses pengamanan data teks menggunakan algoritma modifikasi transposisi columnar?
3. Bagaimana mengimplementasikan dan merancang modifikasi transposisi columnar untuk mengamankan data teks?

1.3 Batasan Masalah

Dari uraian perumusan masalah di atas, agar tidak menyimpang dari tujuan yang diharapkan maaka dibuat beberapa pembatasan masalah antara lain:

1. Data teks yang digunakan dalam format Doc.
2. Batas minimal ukuran Data 2MB.
3. Batas maksimal ukuran panjang kunci 10 karakter.
4. Bahasa pemrograman yang digunakan adalah microsoft visual basic 2008.

1.4 Tujuan Penelitian

Tujuan dari penulisan penelitian ini adalah sebagai berikut :

1. Menjelaskan proses enkripsi dan depenelitian algoritma modfikasi transposisi columnar.
2. Menerapkan algoritma modifikasi transposisi columnar dalam pengamanan data teks.
3. Merancang sebuah aplikasi dan mengimplementasikannya untuk mengamankan data teks menggunakan modifikasi transposisi columnar.

2. LANDASAN TEORI

2.1 Kriptografi

2.1.1 Sejarah Kriptografi

Kriptografi mempunyai sejarah yang panjang dan menakjubkan. Informasi yang lengkap mengenai sejarah kriptografi dapat ditemukan di dalam buku David Kahn yang berjudul The Codebreakers. Buku yang tebalnya 1000 halaman ini menulis secara rinci sejarah kriptografi mulai dari penggunaan kriptografi oleh Bangsa Mesir 4000 tahun yang lalu (berupa hieroglyph yang terdapat pada 10 system) hingga penggunaan kriptografi pada abad ke-20 (Menezes, van Oorschot dan Vanstone, 1996). Secara historis ada empat kelompok yang berkontribusi terhadap perkembangan kriptografi, dimana mereka menggunakan kriptografi untuk menjamin kerahasiaan dalam komunikasi pesan penting, yaitu kalangan militer (termasuk intelijen dan mata-mata), kalangan 10 sytem, penulis buku harian, dan pencinta (lovers). Di antara keempat kelompok ini, kalangan militer yang memberikan kontribusi paling penting karena pengiriman pesan di dalam suasana perang membutuhkan teknik enkripsi dan dekripsi yang rumit.

Sejarah kriptografi klasik mencatat penggunaan cipher transposisi oleh tentara Sparta di Yunani pada permulaan tahun 400 SM. Mereka

ISSN: 2548-9704

menggunakan alat yang namanya scytale. Scytale terdiri dari sebuah kertas panjang dari daun papyrus yang dililitkan pada sebuah silinder dari diameter tertentu (diameter silender menyatakan kunci penyandian). Pesan ditulis secara horizontal, baris per baris. Bila pita dilepaskan, maka huruf-huruf di dalamnya telah tersusun secara acak membentuk pesan rahasia. Untuk membaca pesan, penerima pesan harus melilitkan kembali melilitkan kembali kertas tersebut ke silinder yang diameternya sama dengan diameter silinder pengirim. Sedangkan algoritma substitusi paling awal dan paling sederhana adalah Caesar cipher, yang digunakan oleh raja Yunani kuno, Julius Caesar. Caranya adalah dengan mengganti setiap karakter di dalam 11ystem dengan karakter yang terletak pada tiga posisi berikutnya di dalam susunan alphabet.

Kriptografi modern dipicu oleh perkembangan peralatan 11 system digital.idak seperti kriptografi klasik yang mengenkripsi karakter per karakter (denagn menggunakan alfabet tradisionil), kriptografi modern beroprasi pada string biner. Cipher yang kompleks seperti DES (data encryption standard) dan penemuan algoritma RSA adalah algoritma kriptografi modern yang paling dikenal didalam sejarah kriptografi modern. Kriptografi modern tidak hanya berkaitan dengan teknik menjaga dan serta kerahasiaan pesan, tetapi juga melahirkan konsep seperti tanda-tangan digital dan sertifikat digital. Dengan kata lain, kriptografi modern tidak hanya memberikan aspek keamanan confidentiality.

Selain berdasarkan sejarah yang membagi kriptografi menjadi kriptografi klasik dan kriptografi modren, maka berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan lagi menjadi kriptografi kunci-simetri (symmetric-key cryptography) dan kriptorafi kunci-nirsimetri (asymmetric-key cryptography).

2.1.2 Enkripsi

Enkripsi merupakan bagian dari kriptografi, dan merupakan hal yang sangat penting supaya keamanan data Dekripsi merupakan proses sebaliknya dari enkripsi yaitu mengembalikan sandi-sandi atau informasi yang telah dilacak kebentuk file aslinya dengan menggunakan kunci atau kode yang dikirimkan 7 sytem terjaga kerahasiaannya. Enkripsi 7 sytem diartikan dengan 7 system atau kode, di mana pesan asli (plaintext) diubah menjadi kode-kode tersendiri sesuai metode yang disepakati oleh kedua belah pihak, baik pihak pengirim pesan maupun penerima pesan.

2.1.3 Dekripsi

Dekripsi merupakan proses sebaliknya dari enkripsi yaitu mengembalikan sandi-sandi atau informasi yang telah dilacak kebentuk file aslinya dengan menggunakan kunci atau kode.

2.1.4 Jenis Kriptografi

Kriptografi dapat di bagi menjadi 2 bagian yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik pada umumnya merupakan teknik penyandian dengan kunci simetrik dan menyembunyikan pesan yang memiliki arti ke sebuah pesan yang nampaknya tidak memiliki arti dengan metode subsitusi(pergantian huruf) atau tranposisi (pertukaran tempat). (rifki sadikin , 2012: 15).

Kriptografi modern menggunakan gagasan dasar yang sama seperti kriptografi klasik (permutasi dan transposisi)tetapi penekanannya berbeda. Algoritma kriptografi modern umumnya beroperasi daalam metode bit ketimbang mode karakter (seperti yang dilakukan pada cipher substitusi atau cipher transposisi dari algoritma kriptografi klasik). Operasi dalam mode bit berarti semua data dan informasi (baik kunci,plainteks,maupun cipherteks) dinyatakan dalam rangkaian (string) bit biner, 0 dan 1. Algoritma enkripsi dan dekripsi memproses semua data dan informasi dalam bentuk rangkaian bit. Rangkaian bit yang menyatakan plainteks dienkripsikan menjadi cipherteks dalam bentuk rangkaian bit, demikian sebaliknya.

2.2 Transposisi Columnar

Salah satu sandi transposisi yang paling sederhana adalah sandi transposisi columnar. Cara kerja sandi columnar adalah menulis karakter teks asli dengan orientasi baris dengan panjang karakter yang sama dan kemudian teks sandi didapatkan dengan menulis ulang dengan orientasi kolom. Urutan kolom disepakati sebelumnya untuk mempersulit analisis sandi.

Misalnya ada teks asli “MUNDURSAMPAIBATASKOTA”, maka dengan menulis dalam tabel terdiri dari 6 kolom dengan orientasi baris didapatkan:

Kunci	4	2	1	6	3	5

ISSN: 2548-9704

Teks asli	M	U	N	D	U	R
	S	A	M	P	A	I
	B	A	T	A	S	K
	O	T	A	X	Y	Z

Perhatikan string XYZ pada baris terakhir digunakan untuk mengisi sel kosong pada tabel. Setelah tabel terbentuk tulis teks sandi dengan urutan berdasarkan kunci dengan orientasi kolom. Sehingga didapatkan teks sandi.

NMTAUAATUASYMSBORIKZDPAX

Dekripsi sandi transposisi columnar hampir sama dengan enkripsi namun pada dekripsi jumlah baris dapat dihitung dengan membagi panjang teks sandi dengan panjang kunci. Kemudian isi kolom terlebih dahulu sesuai dengan kunci dengan teks sandi sampai baris terakhir. Teks asli dibaca dari baris pertama sampai baris terakhir.

Implementasi sandi columnar diberikan oleh kode sumber 2.9 sebagai kelas ColumnarCipher. Kelas ColumnarCipher memiliki 2 fungsi: enkripsi dan depenelitian serta sebuah konstuktor yang menetapkan kunci sandi Columnar.

Berikut ini contoh keluaran penggunakan kelas ColumnarCipher:

Teks asli :
MUNDURSAMPAIBATASKOTA
Teks sandi (1X) :
NMTAUAATUASYMSBORIKZDPAX
Teks sandi (2X) :
TUBDMTSZUSRANAMKAYIXAAOP
Teks asli (2X dekripsi) :
MUNDURSAMPAIBATASKOTA.

2.2.1 Perancangan Modifikasi Transposisi Columnar Fungsi Enkripsi

Penulis merancang sebuah fungsi enkripsi sederhana yang terdiri dari 2 tahap, yaitu:

1. Mengacak urutan huruf pada pesan Pengacakan urutan huruf pada pesan dilakukan dengan aturan ganjil-genap. Langkah-langkah implementasi aturan tersebut adalah sebagai berikut:

a. Memisahkan huruf-huruf yang berada pada posisi ganjil dan genap.

b. Melakukan tahap a terhadap huruf-huruf kelompok ganjil dan genap menjadi kelompok ganjilganjil, ganjilgenap, genapganjil, dan genapgenap.

c. Menggabungkan kembali huruf-huruf yang telah terpisah menjadi empat kelompok tersebut dengn aturan ganjilganjilganjilgenap-genapganjil-genapgenap.

2. Meng-inverse urutan huruf setelah diacak Menuliskan posisi huruf dari dari yang paling akhir hingga ke paling awal.

2.2.2 Perancangan Modifikasi Transposisi Columnar Fungsi Dekripsi

Penulis merancang sebuah fungsi dekripsi sederhana yang terdiri dari 2 tahap, yaitu:

1. Meng-inverse urutan huruf Menuliskan posisi huruf dari dari yang paling akhir hingga ke paling awal.

2. Mengacak urutan huruf setelah inverse Mengembalikan posisi huruf ke posisi semula sebelum diacak-acak menggunakan aturan ganjilgenap. Tahapan yang dilakukan adalah:

a. Membagi pesan menjadi 2 bagian sama banyak. Jika jumlah huruf pada pesan adalah ganjil maka bagian pertama berjumlah lebih banyak 1 huruf dibandingkan dengan bagian kedua.

b. Melakukan tahap a terhadap huruf-huruf kelompok pertama dan kedua. Hasil pembagian pada kelompok pertama menjadi bagian 1 dan bagian 2, sedangkan kelompok kedua menjadi bagian 3 dan 4.

c. Menggabungkan keempat bagian yang telah terbentuk diatas pada posisi semula, dimana pada saat enkripsi bagian 1 adalah kelompok ganjilganjil, bagian 2 adalah kelompok ganjilgenap, bagian 3 adalah kelompok genapganjil, dan bagian 4 adalah genapganjil.

3. PEMBAHASAN

3.1 Analisa

Pada bab ini akan membahas mengenai analisa sistem, yaitu meneliti bagaimana proses kerja algoritma tranposisi columnar ini dalam mengamankan dokumen atau data teks, analisa proses enkripsi, analisa proses depenelitian, analisa dan logika yang dibutuhkan untuk menyelesaikan masalah yang ada dalam pengamanan data teks.

3.1.1 Analisa Proses Enkripsi Transposisi Columnar

Cara kerja sandi tranposisi columnar adalah menulis karakter asli dengan orientasi baris dengan panjang karakter yang sama dan kemudian teks sandi didapatkan dengan menulis ulang orientasi kolom. Urutan kolom disepakatin sebelumnya untuk mempersulit analisa sandi

Plainteks : HORMATILAHORANGTUAMU
Kunci : Fauzi → 21453

ISSN: 2548-9704

Proses Enkripsi Transposisi Columnar.

2	1	4	5	3
H	O	R	M	A
T	I	L	A	H
O	R	A	N	G
T	U	A	M	U

Hasilnya chipertext adalah OIRU HTOT AHGU RLAA MANM

3.1.2 Analisa Proses Hasil Dekripsi Tranposisi Columnar

Menjalankan columnar transposition dekripsi dengan menggunakan kata kunci "FAUZI", kita dapat mendekripsikan cipherteks menjadi plainteks.

Pertama, kita tentukan posisi abjad huruf – huruf pada kunci "FAUZI", yaitu 21453.

Kedua, kita bagi cipherteks menjadi 5 bagian.

Tiga, karena kunci terdiri dari 5 huruf. Butuh cara tersendiri untuk menentukan anggota tiap bagian jika jumlah huruf pada pesan bukan merupakan kelipatan dari jumlah huruf pada kunci. Jika kita bagi 20 dan 5 hasilnya adalah 5. Maka hasil pembagiannya adalah sebagai berikut :

Bagian 1 (mewakili huruf 'A') : OIRU
Bagian 2 (mewakili huruf 'F') : HTOT
Bagian 3 (mewakili huruf 'I') : AHGU
Bagian 4 (mewakili huruf 'U') : RLAA
Bagian 5 (mewakili huruf 'Z') : MANM

Empat, kita susun bagian – bagian tersebut dimana tiap bagian membentuk satu kolom dengan huruf – huruf pada kunci diurutkan pada header kolom.

Hasilnya adalah sebagai berikut :

'F'	'A'	'U'	'Z'	'I'
H	O	R	M	A
T	I	L	A	H
O	R	A	N	G
T	U	A	M	U

Setelah itu, kita baca pesan tersebut per row, sehingga didapat plainteks yang dicari, yaitu : "HORMATILAH ORANG TUA MU".

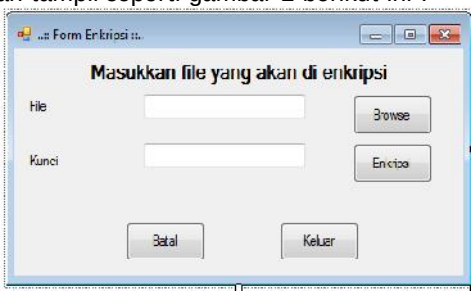
4. ALGORITMA DAN IMPLEMENTASI

Algoritma merupakan kumpulan perintah untuk menyelesaikan suatu masalah. Perintah-perintah ini dapat diterjemahkan secara bertahap dari awal hingga akhir. Masalah tersebut dapat berupa apa saja, dengan catatan untuk setiap masalah, ada kriteria kondisi awal yang harus dipenuhi sebelum menjalankan algoritma.

1. Algoritma Enkripsi
   Input : m ← Plainteks (m)
   K ← Kunci (k)
   Output : C ← Ciphertext (c)
   Proses : E (m) = c
   If E=Enkripsi
   m=Plaintext
   c=ciphertext
   If Plaintext : E (m) = c
   End If
2. Algoritma Dekripsi
   Input : C ← Chipertext (c)
   K ← Kunci (k)
   Output : m ← Plaintext (m)
   Proses : D(c)=m
   IF D= Dekripsi
   m= Plaintext
   C= Chipertext
   If Chipertext : D (c) = m
   End If

Gambar 1 Tampil Layar Utama Menu Enkripsi

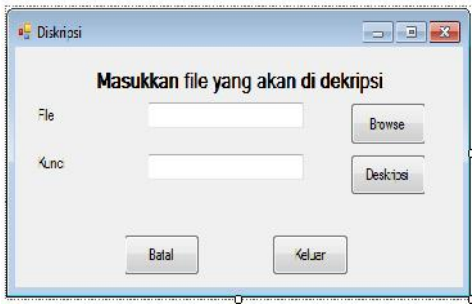
Jika user memilih menu enkripsi maka akan tampil seperti gambar 2 berikut ini :



Gambar 2 Tampilan Layar Enkripsi

Jika user memilih menu dekripsi maka akan tampil seperti gambar 3 berikut ini :

ISSN: 2548-9704



Gambar 3 Tampilan Layar Dekripsi

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah menyelesaikan penelitian dengan judul implementasi algoritma modifikasi transposisi columnar dalam mengamankan data teks, penulis menarik kesimpulan sebagai berikut :

1. Dengan adanya proses enkripsi dan dekripsi algoritma dalam mengamankan data teks dapat memberi kemudahan bagi pengguna untuk mengamankan data yang bersifat rahasia.
2. Pengamanan data teks menggunakan algoritma modifikasi transposisi columnar dapat diterapkan sehingga proses enkripsi dan dekripsi data teks lebih mudah.
3. Aplikasi visual basic dapat mempermudah proses enkripsi dan dekripsi dalam mengamankan data teks.

5.2 Saran

Berdasarkan saran yang dapat dijadikan pertimbanagn dalam mengembangkan penelitian ini adalah :

1. Penulis menyarankan agar program yang dibuat dapat mengenkripsi dan mendekripsi tidak hanya pada dokumen saja melainkan berupa gambar, video.
2. Diharapkan supaya algoritma modifikasi transposisi columnar dapat di kolaborasikan dengan algoritma lain seperti RSA dan DES, agar tingkat proses pengamanan sulit diketahui orang-orang yang tidak berkepentingan.
3. Diharapkan juga aplikasi ini bisa dikembangkan lagi dengan menggunakan bahasa pemrograman lain, seperti aplikasi tools.

DAFTAR PUSTAKA

1. Munir, Rinaldi. 2006. Kriptografi. Bandung: Informatika.
2. Sadikin, Rifki. 2012. Kriptografi. Yogyakarta: Informatika
3. http://Rahimah/1Maret2014/Implementasi-dan-penyandian-pesan-pada-citra-mennggunakan-algoritma-affine-cipher.html.
4. http:// Odit Ekwardo, Modifikasi Columnar Transposisi Menggunakan Sebuah Fungsi Transposisi, ITB Bandung.
5. http://Abdul halim hasugian / Agustus 2013 / ISSN :Implementasi Algoritma Hill Chiper Dalam Mengamankan Data Teks
6. Kadir Abdul,2013: 22
7. Edy Winarto - Ali Zaki, 2013