Paper

Implementasi algoritma Kriptografi Simetris Atbash Cipher dan Teknik Transposisi Segitiga Untuk Pengamanan File Teks

Author: Andy Syahputra, Siti Sundari, Fera Damayanti

ISBN: 978-623-91911-2-2

Implementasi Algoritma Kriptografi Simetris Atbash Cipher Dan Teknik Transposisi Segitiga Untuk Pengamanan File Teks

Andy Syahputra[1], Siti Sundari[2], Fera Damayanti[3]

[1,2,3]Universitas Harapan, Medan, Indonesia

[1]Andisyahputra542@gmail.com, [2] Sundaristth@gmail.com, [3]feradamayantii@gmail.com

Abstrak- Perkembangan teknologi seperti sekarang, dapat mempermudah untuk saling bertukar dan mengirim file, maka diperlukan pengamanan untuk melakukan pencegahan atas sampainya informasi ke tangan yang tidak berhak. Banyak sekali metode pengamanan yang dilakukan untuk menjaga agar dokumen tersebut aman, seperti dengan pemberian sandi isi pesan dan metode lainnya untuk memperkuat keamanan. Pada penelitian ini proses penyandian yang dilakukan adalah dengan menggunakan teknik kriptografi kombinasi algoritma Atbash Cipher dan algoritma Transposisi Segitiga dalam skema super enkripsi. Teknik pengkombinasian antara dua algoritma kriptografi bertujuan untuk mendapatkan ciphertext yang lebih kuat sehingga sulit untuk dipecahkan, dan juga untuk mengatasi penggunaan ciphertext tunggal yang secara komparatif lemah. Untuk mengkombinasikan dua algoritma kriptografi dilakukan dengan cara mengenkripsi file teks terlebih dahulu dengan menggunakan Atbash Cipher yang menghasilkan file terenkripsi yang disebut cipherfile, kemudian mengenkripsi kembali menggunakan teknik Transposisi Segitiga. Untuk mendekripsikan cipherfile, proses yang dilakukan adalah dengan mendekripsikan dengan teknik Transposisi Segitiga terlebih dahulu. Setelah itu kemudian mendekripsikan kembali menggunakan algoritma Atbash Cipher, maka cipherfile kembali ke file asli. Sistem yang dirancang dapat mengenkripsikan pesan berupa file teks berekstensi .txt dan .docx dan mendekripsikannya kembali. Hasil pengujian pada waktu proses berbanding lurus dengan panjang karakter file teks. Artinya semakin panjang file teks yang digunakan maka akan semakin lama juga waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi pada file teks.

Kata Kunci: *Kriptografi, Super Enkripsi, Atbash Cipher, Transposisi Segitiga*

Abstract- The technological developments like now, can make it easier to exchange and send files, it is necessary to take security to prevent the arrival of information into unauthorized hands. There are so many security methods that are used to keep the document safe, such as by giving the message content password and other methods to strengthen security. In this study, the encoding process used is a combination of cryptographic techniques with the Atbash Cipher algorithm and the Triangle Transposition algorithm in a super encryption scheme. The technique of combining two cryptographic algorithms aims to obtain a stronger ciphertext that is difficult to crack, and also to overcome the use of a single ciphertext which is comparatively weak. To combine the two cryptographic algorithms, it is done by first encrypting the text file using the Atbash Cipher which produces an encrypted file called a cipherfile, then re-encrypting it using the Triangle Transposition technique. To decrypt the cipherfile, the process carried out is to decrypt it using the Triangle Transposition technique first. After that, then decrypt again using the Atbash Cipher algorithm, then the cipherfile returns to the original file. The designed system can encrypt messages in the form of text files with .txt and .docx extensions and decrypt them again. The test results at processing time are directly proportional to the character length of the text file. This means that the longer the text file used, the longer it will take to encrypt and decrypt the text file.

Keywords: *Cryptography, Super Encryption, Atbash Cipher, Transposisi Segitiga*

1. PENDAHULUAN

Pada saat ini dokumen menjadi hal yang sangat penting dalam urusan sehari-hari, karena dokumen merupakan benda yang dapat digunakan sebagai bukti atau keterangan. Seiring dengan perkembangan teknologi, muncul dokumen dalam bentuk elektronik yang dapat diakses diberbagai macam media elektronik, misalnya komputer. Dokumen elektronik mempunyai ekstensi file sebagai tanda yang membedakan jenis-jenis dari file. Contoh ekstensi file yaitu .doc dan .txt. Ekstensi file .doc sendiri merupakan singkatan dari document, adalah ekstensi file yang biasa diakses melalui Microsoft Word. Sedangkan .txt adalah ekstensi file yang tidak terformat seperti yang ada pada Microsoft Word. Perangkat lunak yang biasa digunakan untuk memanipulasi format data .txt adalah Notepad.

ISBN: 978-623-91911-2-2

Adanya perkembangan teknologi seperti sekarang, dapat mempermudah untuk saling bertukar dan mengirim file. Bertukar file dapat bersifat umum dan pribadi, yang dimaksud dengan umum adalah ketika penerima file yang dituju adalah orang banyak atau lebih dari satu. Sedangkan yang bersifat pribadi yaitu, penerima file dikhususkan hanya kepada penerima yang dikehendaki pengirim saja. Jadi, agar file tersebut dapat terjaga keamanan dan keasliannya serta menghindari kerusakan dari pihak luar yang tidak bersangkutan hingga file dapat sampai kepada penerima yang dituju oleh pengirim, maka diperlukan pengamanan untuk melakukan pencegahan atas sampainya informasi ke tangan yang tidak berhak.

Banyak sekali metode pengamanan yang dilakukan untuk menjaga agar dokumen tersebut aman, seperti dengan pemberian sandi isi pesan dan metode lainnya untuk memperkuat keamanan. Pada penelitian ini proses penyandian yang dilakukan adalah dengan menggunakan teknik kriptografi. Kriptografi adalah ilmu yang mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat tulisan tersebut tidak dapat dibaca oleh orang yang tidak berkepentingan [1]. Kriptografi merupakan salah satu sistem keamanan dengan konsep membuat data menjadi sandi-sandi yang tidak setiap orang dapat membacanya [2]. Kriptografi bertujuan menjaga kerahasian informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah [3]. Kriptografi melingkupi proses transformasi informasi menjadi suatu bentuk yang tidak dapat dipahami, sehingga orang-orang yang tidak berhak tidak mungkin mengerti. Proses transformasi tersebut terdiri dari enkripsi dan dekripsi. Enkripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode atau data dari yang biasa dimengerti, disebut *Plaintext* , menjadi sebuah kode yang tidak bisa dimengerti, disebut dengan ciphertext. Sedangkan proses kebalikannya untuk mengubah ciphertext menjadi *Plaintext* disebut dekripsi [4].

Pada penelitan ini akan mengimplementasikan kombinasi algoritma Atbash Cipher dan algoritma teknik Transposisi Segitiga untuk pengamanan file teks. Algoritma Atbash adalah cipher substitusi dengan cara membalikkan alfabet sehingga setiap huruf dipetakan ke huruf di posisi yang sama kebalikan dari abjad. Pada model penyandian ini, huruf "A" pada *Plaintext* diubah menjadi huruf "Z" pada ciphertext, huruf "B" akan disandikan dengan huruf "Y", dan seterusnya [5]. Teknik Transposisi Segitiga memiliki pola pada baris pertama dimulai dari satu karakter dan baris selanjutnya bertambah 2 karakter dari baris sebelumnya. Bentuk ini memberi pola bilangan ganjil baris pertama 1 karakter, baris kedua 3 karakter, baris ketiga 5 karakter dan selanjutnya. Pola ini tergantung banyak digit dari *Plaintext* yang akan ditransposisikan. Untuk enkripsi, pola ini ditulis per baris dimulai dari baris paling atas, kemudian dibaca per kolom yang dimulai dari kolom paling kiri untuk menghasilkan ciphertext [6].

Metode pengkombinasian antara kedua algoritma bertujuan untuk mendapatkan ciphertext yang lebih kuat sehingga sulit untuk dipecahkan, dan juga untuk mengatasi penggunaan ciphertext tunggal yang secara komparatif lemah. Metode penggabungan dua algoritma enkripsi ini disebut dengan super enkripsi. Berdasarkan uraian yang dikemukakan diatas, maka penulis mencoba mengangkat topik tugas akhir dengan judul penelitian "Implementasi Algoritma Kriptografi Simetris Atbash Cipher dan Teknik Transposisi Segitiga Untuk Pengamanan File Teks".

2. METODE PENELITIAN

Pada penelitan ini akan mengimplementasikan kombinasi algoritma kriptografi Atbash Cipher dan algoritma kriptografi dengan teknik Transposisi Segitiga untuk pengamanan file teks. Metode pengkombinasian antara kedua algoritma yang bertujuan untuk mendapatkan ciphertext yang lebih kuat sehingga sulit untuk dipecahkan, dan juga untuk mengatasi penggunaan ciphertext tunggal yang secara komparatif lemah. Metode penggabungan dua algoritma enkripsi ini disebut dengan super enkripsi.

Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim kesuatu tempat ke tempat lain [6]. Tujuan dari kriptografi adalah untuk melindungi data yang ditransmisikan dalam kemungkinan adanya penyalahgunaan data, sehingga kriptografi adalah prosedur dimana data teks biasa disamarkan, atau dienkripsi, menghasilkan teks yang diubah, yang disebut ciphertext. Ciphertext dapat diubah secara terbalik oleh penerima yang ditunjuk sehingga *Plaintext* asli dapat dipulihkan [2]. Terdapat dua jenis algoritma kriptografi berdasar jenis kuncinya yaitu algoritma simetris (konvensional) dan algoritma asimetris (kunci-publik). Kriptografi simteris atau disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi [7]. Proses enkripsi pada kriptografi simetris sangat baik namun sangat rentan pada pengamanan datanya yang dienkripsi [8]. Ada beberapa kelebihan menggunakan kunci simetris yang sudah diketahui yaitu Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetris walupun hal ini berbanding lurus dengan penambahan ukuran file, kecepatan proses enkripsi/dekripsi bergantung pada besarnya ukuran file, semakin besar ukuran file semakin banyak waktu yang dibutuhkan untuk enkripsi/dekripsi [7].

Kunci asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi [7]. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibanding enkripsi simetris, karena enkripsi asimetris menggunakan bilangan-bilangan yang sangat besar. Namun enkripsi asimetris lebih lama dibanding enkripsi

ISBN: 978-623-91911-2-2

simetris [8]. Teknik enkripsi asimetris ini jauh lebih lambat ketimbang enkripsi dengan kunci simetris. Oleh karena itu, biasanya bukanlah pesan itu sendiri yang disandikan dengan kunci asimetris, namun hanya kunci simetrislah yang disandikan dengan kunci asimetris. Sedangkan pesannya dikirim setelah disandikan dengan kunci simetris [7].

Algoritma Atbash adalah cipher substitusi sederhana dengan cara membalikkan alfabet sehingga setiap huruf dipetakan ke huruf di posisi yang sama kebalikan dari abjad [5]. Sandi Atbash digunakan bangsa Yahudi sekitar 600 SM (Sebelum Masehi). Sandi Atbash mengganti alfabet Hebrew dengan korespondensi kebalikannya. Jika diterapkan pada alfabet latin [3], maka akan berupa:

Pi : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Ci : Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Maka dari penerapan pada alfabet menghasilkan rumus enkripsi dan dekripsi [5] dengan menggunakan persamaan (1).

$$E(x) = D(x) = (-x \; mod \; m) + 1 \quad (1)$$

Keterangan:

E (x) : proses enkripsi
D (x) : proses dekripsi
x : *Plaintext* atau ciphertext
m : jumlah alfabet dari A-Z

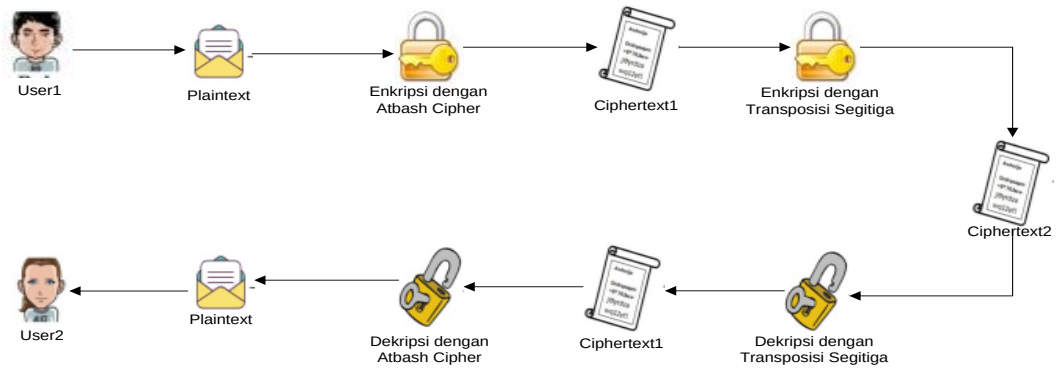
Pada model penyandian ini, huruf "A" pada *Plaintext* diubah menjadi huruf "Z" pada ciphertext, huruf "B" akan disandikan dengan huruf "Y", dan seterusnya [5]. Pada Atbash Cipher rumus enkripsi dan dekripsi sama, dimana x diganti dengan nilai desimal karakter yang akan dienkripsi atau didekripsi dan m pada rumus Atbash Cipher diganti dengan angka 26, dimana angka 26 merupakan jumlah seluruh karakter.

Teknik Transposisi Segitiga memiliki pola pada baris pertama dimulai dari satu karakter dan baris selanjutnya bertambah 2 karakter dari baris sebelumnya. Bentuk ini memberi pola bilangan ganjil baris pertama 1 karakter, baris kedua 3 karakter, baris ketiga 5 karakter dan selanjutnya. Pola ini tergantung banyak digit dari *Plaintext* yang akan ditransposisikan. Untuk enkripsi, pola ini ditulis per baris dimulai dari baris paling atas, kemudian dibaca per kolom yang dimulai dari kolom paling kiri untuk menghasilkan ciphertext [6]. Tidak seperti cipher substitusi sederhana (seperti Caesar Cipher), yang mengubah huruf pesan di sekitar, Transposisi Ciphers malah bekerja dengan mengotak-atik urutan huruf untuk menyembunyikan pesan yang sedang dikirim. Model operasi algoritma ini mirip dengan anagram, namun dengan struktur yang lebih teratur sehingga bisa didekripsi dengan mudah [2].

File teks merupakan berkas yang mengandung informasi-informasi dalam bentuk teks yang terdiri dari karakter, angka dan tanda baca. Data yang berasal dari dokumen pengolah kata, angka yang digunakan dalam perhitungan, nama dan alamat dalam basis data merupakan contoh masukan data teks yang terdiri dari karakter, angka dan tanda baca. Contoh format data teks di atas beserta perangakat lunak yang biasa digunakan adalah *.txt dan *.doc. Format data teks merupakan format teks yang digunakan untuk menyimpan huruf, angka, karakter kontrol (tabulasi, pindah baris, dan sebagainya) atau symbol-simbol lain yang biasa digunakan dalam tulisan seperti titik, koma, tanda petik, dan sebagainya. Kelebihan dari format data teks ini adalah ukuran datanya yang kecil karena tiada fitur untuk memformat tampilan teks. Saat ini perangkat lunak yang paling banyak digunakan untuk memanipulasi format data ini adalah Notepad. Doc merupakan ekstensi arsip dokumen perangkat lunak Microsoft Word yang paling banyak digunakan dalam menulis laporan, makalah dan sebagainya. Doc merupakan jenis teks terformat yang tidak hanya dapat mengatur tampilan teks seperti styles (font, ukuran huruf, dan sebaginya), namun juga dapat menyisipkan gambar. Kekurangan format teks dokumen ini terletak pada ukuran datanya yang besar [9].

Arsitektur umum sistem merupakan skema perancangan sistem yang mendekripsikan alur sistem secara keseluruhan. Arsitektur umum sistem juga dapat menjadi pedoman untuk pembuatan pemodelan sistem. Adapun arsitektur umum sistem enkripsi file teks dapat dilihat pada gambar 1.

ISBN: 978-623-91911-2-2



Gambar 1. Arsitekur Umum Sistem

Dapat dilihat pada gambar 1 menjelaskan bahwa proses enkripsi antara *Plaintext* dan algoritma kriptografi Atbash Cipher yang dilakukan oleh user1 akan menghasilkan ciphertext1. Selanjutnya user1 akan melakukan proses enkripsi antara ciphertext1 yang dihasilkan dengan teknik Transposisi Segitiga yang kemudian menghasilkan ciphertext2. Proses selanjutnya adalah proses dekripsi oleh user2 antara ciphertext2 dengan teknik Transposisi Segitiga yang menghasilkan kembali ciphertext1. Proses yang terakhir adalah proses dekripsi yang dilakukan oleh user2 antara ciphertext1 dengan algoritma Atbash Cipher yang menghasilkan *Plaintext* semula yang dikirimkan oleh user1.

3. HASIL DAN PEMBAHASAN

Proses enkripsi file teks pada tahap pertama dimulai dengan menggunakan algoritma Atbash Cipher untuk mendapatkan ciphertext. Atbash Cipher merupakan suatu teknik enkripsi, dimana huruf alphabet disubtitusi dengan kebalikannya. Maksud dari kebalikan disini adalah huruf awal diganti dengan huruf terakhir, huruf kedua diganti dengan sebelum terakhir, dan seterusnya. Pada model penyandian Atbash Cipher, huruf "A" pada *Plaintext* diubah menjadi huruf "Z" pada ciphertext, huruf "B" akan disandikan dengan huruf "Y", dan seterusnya. Pada algoritma Atbash Cipher rumus untuk enkripsi dan dekripsi sama dengan menggunakan persamaan (2.3), dimana x diganti dengan nilai desimal karakter yang akan dienkripsi atau didekripsi dan m pada rumus Atbash Cipher diganti dengan angka 26, dimana angka 26 merupakan jumlah seluruh karakter. Berikut ini adalah tabel substitusi yang disusun bedasarkan algoritma Atbash Cipher seperti disajikan pada tabel 1.

Tabel 1. Atbash Cipher Dalam Bentuk Angka

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Dari tabel 1 bisa dilihat bahwa terdapat alphabet mulai dari A sampai Z dalam bentuk angka, nantinya angka-angka tersebut akan dijumlahkan untuk keperluan mengenkripsi dan dekripsi pada algoritma Atbash Cipher. Misalnya diketahui sebuah pesan teks yaitu sebagai berikut:

Pesan Tesk (*Plaintext*) : PRODI TEKNIK INFORMATIKA

Maka proses perhitungan enkripsi algoritma Atbash Cipher dengan menggunakan persamaan (1), yaitu pertama ubah nilai karakter pesan teks kedalam nilai desimal Atbash Cipher, berdasarkan tabel 1 didapat nilai desimal Atbash Cipher dari karakter pesan teks yaitu seperti disajikan pada tabel 2.

Tabel 2. Konversi *Plaintext* Atbash Cipher

P	**R**	**O**	**D**	**I**	**T**	**E**	**K**	**N**	**I**	**K**	**I**	**N**	**F**	**O**	**R**	**M**	**A**	**T**	**I**	**K**	**A**
16	18	15	4	9	20	5	11	14	9	11	9	14	6	15	18	13	1	20	9	11	1

Tabel 2 merupakan hasil konversi *Plaintext* kedalam bentuk angka dalam alphabet yang digunakan pada algoritma Atbash Cipher. Dengan menggunakan rumus enkripsi pada persamaan (1).

$E(P) = (-P \ mod \ 26) + 1 = (-16 \ mod \ 26) + 1 = 11$

$E(R) = (-R \ mod \ 26) + 1 = (-18 \ mod \ 26) + 1 = 9$

$E(O) = (-O \ mod \ 26) + 1 = (-15 \ mod \ 26) + 1 = 12$

ISBN: 978-623-91911-2-2

Lakukan hal yang sama sampai semua *Plaintext* berhasil di enkripsi, sehingga didapat nilai desimal Atbash Cipher: 11 9 12 23 18 7 22 16 13 18 16 18 13 21 12 9 14 26 7 18 16 26, dan jika diubah ke karakter berdasarkan tabel 1 maka diperoleh ciphertext seperti terlihat pada tabel 3.

Tabel 3. Konversi Ciphertext Atbash Cipher

Plaintext																					
P	R	O	D	I	T	E	K	N	I	K	I	N	F	O	R	M	A	T	I	K	A
1	1	1	4	9	2	5	1	1	9	1	9	1	6	1	1	1	1	2	9	1	1
6	8	5			0		1	4		1		4		5	8	3		0		1	
Ciphertext																					
K	I	L	W	R	G	V	P	M	R	P	R	M	U	L	I	N	Z	G	R	P	Z
1	9	1	2	1	7	2	1	1	1	1	1	1	2	1	9	1	2	7	1	1	2
1		2	3	8		2	6	3	8	6	8	3	1	2		4	6		8	6	6

Berdasarkan tabel 3 maka hasil enkripsi *Plaintext* "PRODI TEKNIK INFORMATIKA" akan menghasilkan ciphertex "KILWRGVPMRPRMULINZGRPZ".

Ciphertext dari hasil enkripsi algoritma Atbash Cipher selanjutnya akan di enkripsi lagi untuk tahap ke dua dengan menggunakan kriptografi teknik Transposisi Segitiga. Transposisi Segitiga memiliki pola pada baris pertama dimulai dari satu karakter dan baris selanjutnya bertambah 2 karakter dari baris sebelumnya. Bentuk ini memberi pola bilangan ganjil baris pertama 1 karakter, baris kedua 3 karakter, baris ketiga 5 karakter dan selanjutnya. Pola ini tergantung banyak digit dari *Plaintext* yang akan ditransposisikan. Untuk enkripsi, pola ini ditulis per baris dimulai dari baris paling atas, kemudian dibaca per kolom yang dimulai dari kolom paling kiri untuk menghasilkan ciphertext.

Input data sebagai *Plaintext* algoritma Transposisi Segitiga yaitu ciphertext dari algoritma Atbash Cipher, sehingga hasil enkripsinya dapat dijelaskan pada tabel 4.

Tabel 4. Proses Enkripsi Transposisi Segitiga

				K				
			I	L	W			
		R	G	V	P	M		
	R	P	R	M	U	L	I	
N	Z	G	R	P	Z	#	#	#

Dari gambar 4 dapat dilihat hasil transposisi yang dilakukan dengan *Plaintext* yang diberikan. Jika karakter tidak memenuhi semua kolom pada baris terakhir maka akan dimasukkan karakter # sebagai pengisinya. Untuk membaca hasil transposisi terlebih dahulu dibaca dari kolom paling kiri, sehingga hasil enkripsi (*ciphertext*) Transposis Segitiga yang didapat yaitu: NRZRPGIGRRKLVMPWPUZML#I##.

Berdasarkan hasil enkripsi dengan mengkombinasikan algortima Atbash Cipher dengan teknik Transposisi Segitiga dalam skema super enkripsi dalam mengenkripsi *Plaintext* "PRODI TEKNIK INFORMATIKA", maka diperoleh hasil enkripsi (ciphertext) "NRZRPGIGRRKLVMPWPUZML#I##".

Proses dekripsi file teks pada tahap pertama dimulai dengan menggunakan algoritma Transposisi Segitiga. Untuk mengembalikan *Plaintext* yang telah ditransposisi, dilakukan penyusunan kembali karakter kedalam segitiga, dengan karakter pertama menduduki kolom paling kiri dan dibaca dari baris atas ke bawah, maka hasil ciphertext dapat dilihat pada tabel 5.

Tabel 5. Proses Dekripsi Transposisi Segitiga

				K				
			I	L	W			
		R	G	V	P	M		
	R	P	R	M	U	L	I	
N	Z	G	R	P	Z	#	#	#

Berdasarkan gambar 5 dari proses dekripsi Transposisi Segitiga maka diperoleh hasilnya adalah "KILWRGVPMRPRMULINZGRPZ###", dan setiap karakter "#" akan dihapus dari sehingga menghasilkan *Plaintext* "KILWRGVPMRPRMULINZGRPZ".

Plaintext dari hasil dekripsi algoritma Transposisi Segitiga selanjutnya akan di dekripsi lagi untuk tahap ke dua dengan menggunakan kriptografi algoritma Atbash Cipher. Proses dekripsi algoritma Atbash Cipher dengan menggunakan persamaan (2.3), yaitu pertama ubah nilai karakter *Plaintext* (hasil dekripsi Transposisi Segitiga)

ISBN: 978-623-91911-2-2

kedalam nilai desimal Atbash Cipher, berdasarkan tabel 3.6 didapat nilai desimal Atbash Cipher dari karakter *Plaintext* yaitu dapat dijelaskan pada tabel 6.

Tabel 6. Konversi *Plaintext* (Hasil Dekripsi Transposisi Segitiga) Atbash Cipher

K	**I**	**L**	**W**	**R**	**G**	**V**	**P**	**M**	**R**	**P**	**R**	**M**	**U**	**L**	**I**	**N**	**Z**	**G**	**R**	**P**	**Z**
11	9	12	23	18	7	22	16	13	18	16	18	13	21	12	9	14	26	7	18	16	26

Tabel 6 merupakan hasil konversi *Plaintext* (hasil dekripsi Transposisi Segitiga) kedalam bentuk angka dalam alphabet yang digunakan pada algoritma Atbash Cipher. Dengan menggunakan rumus dekripsi pada persamaan (1).

$D(K) = (-K \ mod \ 26) + 1 = (-11 \ mod \ 26) + 1 = 16$
$D(I) = (-I \ mod \ 26) + 1 = (-9 \ mod \ 26) + 1 = 18$
$D(L) = (-L \ mod \ 26) + 1 = (-12 \ mod \ 26) + 1 = 15$

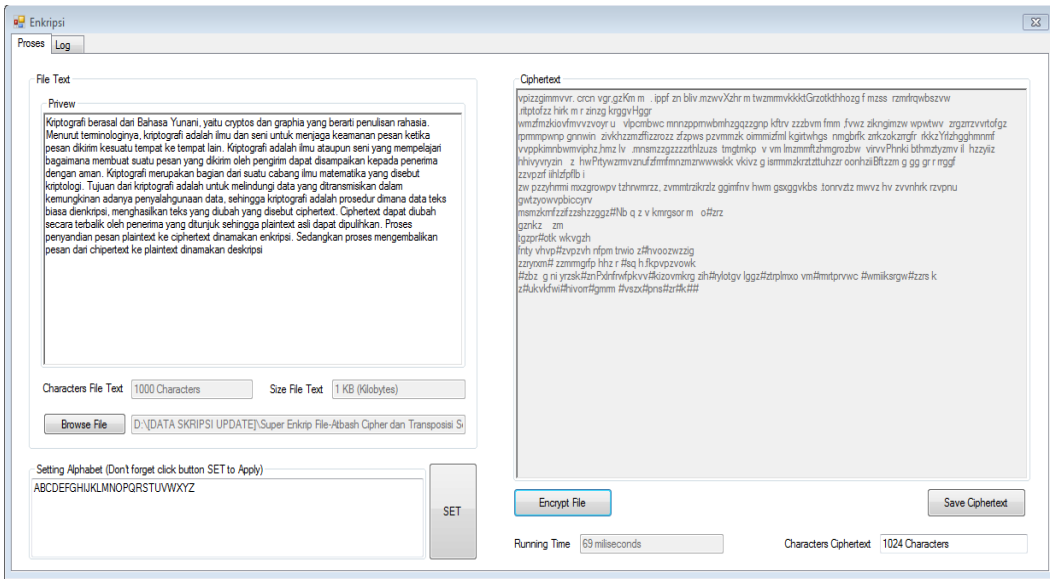
Lakukan hal yang sama sampai semua ciphertext berhasil di dekripsi, maka didapat nilai desimal Atbash Cipher: 16 18 15 4 9 20 5 11 14 9 11 9 14 6 15 18 13 1 20 9 11 1, dan jika diubah ke karakter berdasarkan tabel 3.1 maka diperoleh *Plaintext* seperti terlihat pada tabel 7.

Tabel 7. Konversi Hasil Dekripsi Atbash Cipher

										Ciphertext											
K	I	L	W	R	G	V	P	M	R	P	R	M	U	L	I	N	Z	G	R	K	Z
1	9	1	2	1	7	2	1	1	1	1	1	1	2	1	9	1	2	7	1	1	2
1		2	3	8		2	6	3	8	6	8	3	1	2		4	6		8	1	6
										Plaintext											
P	R	O	D	I	T	E	K	N	I	K	I	N	F	O	R	M	A	T	I	K	A
1	1	1	4	9	2	5	1	1	9	1	9	1	6	1	1	1	1	2	9	1	1
6	8	5			0		1	4		1		4		5	8	3		0		1	

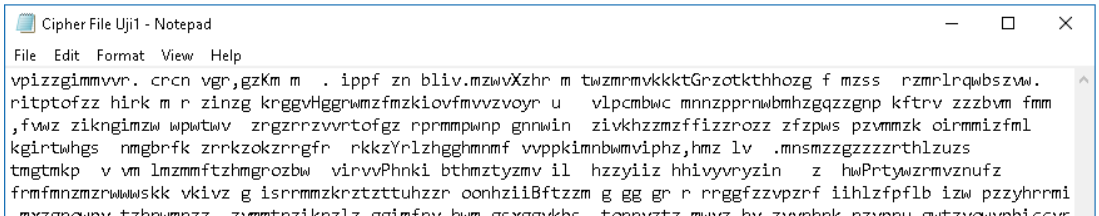
Hasil dekripsi ciphertext pada tabel 1 akan menghasilkan *Plaintext* "PRODI TEKNIK INFORMATIKA" yang sama persis dengan pesan aslinya.

Pengujian proses enkripsi dan dekripsi dilakukan terhadap dua buah kasus. Pertama adalah terhadap file teks berekstensi .txt dan yang kedua terhadap file teks dengan ekstensi .doc.



Gambar 2. Proses Enkripsi File Teks

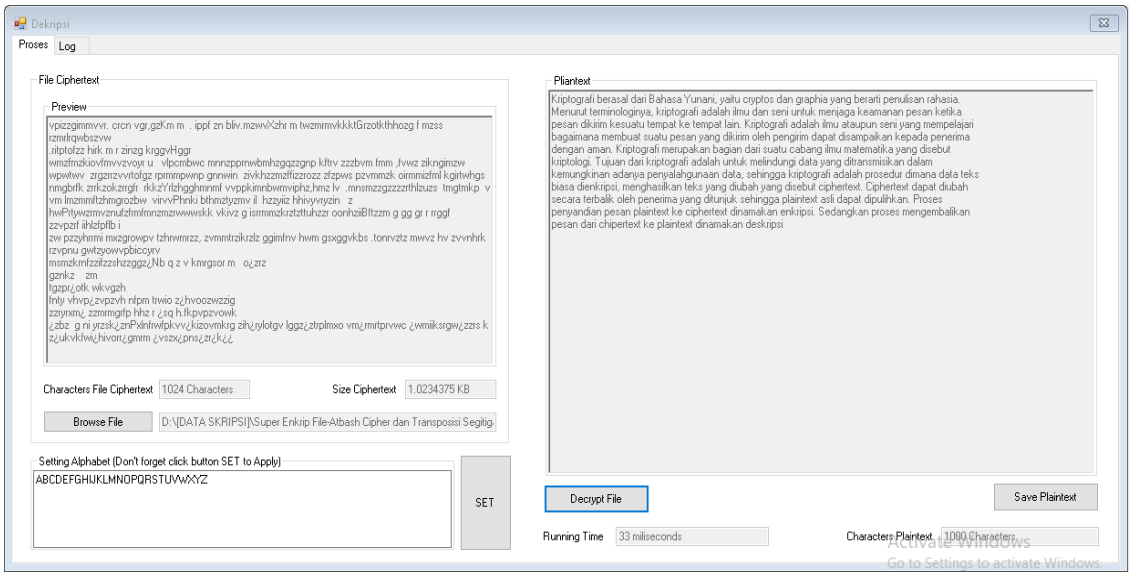
Gambar 2 merupakan tampilan dari proses enkripsi terhadap file teks berekstensi .txt dengan jumlah karakter sebanyak 1000 karakter dengan ukuran 0,986 KB. Adapun tampilan hasil enkripsi file teks setelah berhasil di enkripsi dengan menggunakan algoritma Atbash Cipher dan Transposisi Segitiga dapat disajikan pada gambar 3.



ISBN: 978-623-91911-2-2

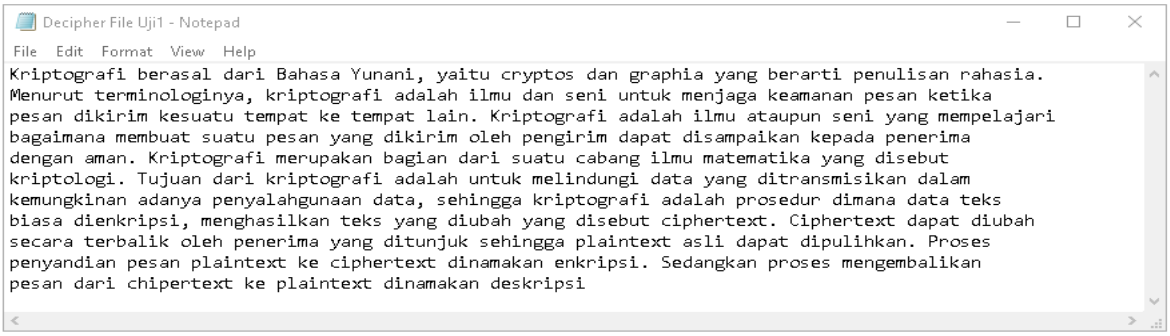
Gambar 3. Preview Hasil Enkripsi File Teks

Setelah file teks berhasil di enkripsi, maka tahap selanjutnya dilakuan pengujiann proses dekripsi untuk mengembalikan ciphertext ke pesan aslinya (*Plaintext*).



Gambar 4. Proses Dekripsi File Teks

Adapun tampilan hasil dekripsi file teks dengan ekstensi .txt setelah berhasil di dekripsi dengan menggunakan algoritma Atbash Cipher dan Transposisi Segitiga dapat disajikan pada gambar 5.



Gambar 5. Hasil Deskripsi File Teks

4. KESIMPULAN

Kesimpulan yang dapat diambil setelah melaukan implementasi dan pengujian sistem terhadap pengaman file teks yang menerapkan algoritma Atbash Cipher dan teknik Transposisi Segitiga adalah sebagai berikut:

ISBN: 978-623-91911-2-2

1. Metode Kombinasi algoritma Atbash Cipher dan teknik Transposisi Segitiga dalam skema super enkripsi berhasil diterapkan untuk pengamanan file teks dengan cara mengenkripsi file dan mengembalikannya seperti semula dengan proses dekripsi tanpa ada kekurangan dan perbedaan karakter dan ukuran pada file.
2. Sistem yang dirancang dapat mengenkripsikan pesan berupa file teks berekstensi .txt dan .docx dan mendekripsikannya kembali. Hasil pengujian pada waktu proses diperoleh bahwa waktu proses algoritma berbanding lurus dengan panjang karakter file teks. Artinya semakin panjang file teks yang digunakan maka akan semakin lama juga waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi pada file teks tersebut.
3. Teknik pengkombinasian antara dua algoritma kriptografi dalam skema super enkripsi bertujuan untuk mendapatkan ciphertext yang lebih kuat sehingga sulit untuk dipecahkan, dan juga untuk mengatasi penggunaan ciphertext tunggal yang secara komparatif lemah. Untuk mengkombinasikan dua algoritma kriptografi dilakukan dengan cara mengenkripsi file teks terlebih dahulu dengan menggunakan Atbash Cipher yang menghasilkan file terenkripsi yang disebut cipherfile, kemudian mengenkripsi kembali menggunakan teknik Transposisi Segitiga. Untuk mendekripsikan cipherfile, proses yang dilakukan adalah dengan mendekripsikan dengan teknik Transposisi Segitiga terlebih dahulu. Setelah itu kemudian mendekripsikan kembali menggunakan algoritma Atbash Cipher, maka cipherfile kembali ke file asli**.**

DAFTAR PUSTAKA

[1] Meliala, Steven Aditya. 2019. Perancangan Aplikasi Pengkodean dan Penyembunyian Pesan Didalam Media Citra Dengan Menggunakan Algoritma Atbash Cipher dan Metode Bit Plane Complexity Segmentation. Jurnal Pelita Informatika, Vol. 7, No. 3.

[2] Sinaga, Daurat, et al. 2018. Teknik Super Enkripsi Menggunakan Transposisi Kolom Berbasis Vigenere Cipher Pada Citra Digital. Jurnal Dinamika Rekayasa Vol. 14, No. 1.

[3] Situmorang, Benny Hermanto, et al. 2018. Implementasi Algoritma Atbash Untuk Menyandikan Pesan Teks Berbasis Android. Jurnal Pelita Informatika, Vol. 7, No. 2.

[4] Zamara, Shabrizqi. 2019. Penerapan Algoritma Vegenere Cipher dan Vernam Cipher Dalam Penggamanan File Text. Jurnal Riset Komputer (JURIKOM), Vol. 6, No. 3.

[5] Afandi, Muhammad Iqbal & Nurhayati. 2020. Implementasi Algoritma Vigenere Cipher Dan Atbash Cipher Untuk Keamanan Teks Pada Aplikasi Catatan Berbasis Android. IT Journal, Vol. 8, No. 1.

[6] Nurhasanah, et al. 2017. Implementasi Operasi XOR dan Teknik Transposisi Segitiga untukPengamanan Citra JPEG Berbasis Android. Jurnal Ilmiah Core IT, Vol. 5, No. 2.

[7] Basri. 2016. Kriptografi Simetris dan Asimetris Dalam Perspektif Keamanan Data dan Kompleksitas Komputasi. Jurnal Ilmiah Ilmu Komputer, Vol. 2, No. 2.

[8] Jamaludin. 2018. Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem. Publikasi Jurnal & Penelitian Teknik Informatika, Vol. 2, No. 2.

[9] Subada, Mhd. Ali. 2018. Analisis Perbandingan Algoritma Even-Rodeh Code dan Algoritma Fibonacci Code Untuk Kompresi File Teks. Fakultas Ilmu Komputer Dan Teknologi Informasi Universitas Sumatera Utara.