Jurnal Sistem Komputer dan Informatika (JSON)
Volume 3, Nomor 1, September 2021
e-ISSN 2685-998X
DOI 10.30865/json.v3i1.2630

Penerapan Modifikasi Algoritma Trithemius Pada Aplikasi Penyimpanan File Secara Online

Andriaman Purba, Nelly Astuti Hasibuan

Fakultas Ilmu Komputer dan Teknologi Informasi, Prodi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: [1]andripurba329@gmail.com
Submitted: **03/12/2020**; Accepted: **15/09/2021**; Published: **30/09/2021**

Abstrak–Semakin berkembangnya zaman maka semakin luas pula pengetahuan, begitu juga dengan hal penyimpanan file. Seperti diketahui pada saat ini sangat banyak masyarakat menyimpan file secara online karena mudah di akses kapan saja dan dimana saja hanya dengan bermodal jaringan, namun kekurangan dari penyimpanan online yaitu akan hal keamanan yang dapat meresahkan pengguna pada setiap alikasi penyimpanan online. Maka dengan penulis menggunakan salah satu Algoritma Kriptografi yaitu Modifikasi Algoritma Trithemius untuk melakuakan keamanan file yang disimpan pada media online. Algoritma ini dapat mengubah kode dengan melakukan enkripsi terhadap file. Diharapkan masyarakat menerapkan atau menggunakan modifiksi Algoritma Trithemius agar dapat membantu masyarakat dalam mengamankan file khususnya file penting.

Kata Kunci: File; Kriptografi; Trithemius

Abstract–The more time is developing, the more knowledgeable, as well as file storage. As is known at this time very many people save files online because it is easy to access anytime and anywhere only with capital, but the drawback of online storage is the security that can be unsettling to users at any point of online storage. So the authors use one of the Cryptographic Algorithms, namely the Modification of the Trithemius Algorithm to carry out the security of files stored on online media. This algorithm can change the code by encrypting files. It is hoped that the community will apply or use the Trithemius Algorithm modification in order to help the community in securing files, especially important files.

Keywords: File; Cryptography; Trithemius

1. PENDAHULUAN

Seiring dengan berkembangnya zaman maka teknologi dan media digital juga mengalami perkembangan dan perubahan yang sangat besar. Begitu pula dengan fungsi internet, seperti yang diketahui bahwa internet sudah banyak digunakan dikehidupan sehari-hari seperti sebagai sarana dalam mendapatkan informasi karena semua informasi bisa didapatkan secara online. Perkembangan teknologi juga sudah mencapai kemedia penyimpanan file secara online, sebagai contoh yang sering digunakan banyak orang yaitu kumpul bagi, google drive, dropbox, OneDrive dan masih banyak lagi.

Dalam melakukan penyimpanan file secara online masih ada satu hal yang harus diperhatikan yaitu masalah keamanan. Karena file yang diunggah secara online dapat diakses orang banyak sehingga jika ada file penting yang akan disimpan dalam media penyimpanan online harus dilakukan proses pengamanan sehingga file yang diupload menjadi lebih aman. Salah satu cara untuk mengamankan yaitu dengan menerapkan suatu algoritma kriptografi yang merupakan ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman.

Hasil penelitian sebelumnya yang dilakukan oleh Arif Prayitno dan Nurdin pada tahun 2017 pada tahun 2012 telah berhasil melakukan pembuktian terhadap pengamanan pesan. Pada penelitian tersebut, penulis berhasil mengamankan pesan dengan menggunakan algoritma Cipher Transposition dan penulis pada penelitian juga menyimpulkan bahwa algoritma tersebut dapat mengembalikan file citra dari hasil proses enkripsi-penyisipan seperti semula[1].

Yuri Prihantono dan Gusari Bagio juga menjelaskan penelitiannya pada tahun 2016 tentang pengamanan file sebagai solusi keamanan data pada smartphone berbasis android dimana penelitian mereka memiliki fitur keamanan aplikasi dengan menggunakan PIN/passcode tersebut dimasukkan pada setiap aplikasi yang dijalankan dengan tujuan agar aplikasinya hanya dapat dijalankan oleh orang yang memiliki akses[2].

Maka dengan itu penulis menyarankan suatu solusi dalam mengamankan file yang disimpan dalam penyimpanan file melalui aplikasi penyimpanan file secara online yaitu dengan melakukan penerapan Algoritma Trithemius. Algoritma Trithemius yang digunakan pada aplikasi penyimpanan file secara online berfungsi untuk mengamankan file yang disimpan denagn mengubah atau menghasilkan suatu kode baru, sehingga file tersebut tidak dapat diakses atau diambil orang yang tidak berkepentingan.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata kriptografi dibagi menjadi dua, yaitu *crypto* dan *graphia* yang berarti penulisan rahasia (tulisan). Kriptografi (*Cryptography*) adalah ilmu ataupun dapat juga disebut seni yang mempelajari teknik bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 3, Nomor 1, September 2021
e-ISSN 2685-998X
DOI 10.30865/json.v3i1.2630

disampaikan kepada penerima dengan aman[3]. Secara singkat dapat dituliska bahwa kriptografi adalah ilmu yang mempelajari penulisan data secara rahasia.

2.2 Algotitma Trithemius

Algoritma Trithemius merupakan kelanjutan dari *cipher polyalphabetic* oleh Albert dimana Johannes Trithemius memanfaatkan sebuah tabel alfabet untuk membantu dalam enkripsi dan dekripsi *cipher polyalphabetic*[4]. Pada proses enkripsi, huruf selanjutnya pada *plaintext* akan digantikan dengan huruf yang relevan dari baris berikutnya pada tabel. Setelah menggunakan baris terakhir, salah satu harus pindah kembali ke baris pertama. sehingga dapat dijelaskan bahwa semua huruf pada *plaintext* akan berubah sesuai dengan jumlah posisi yang ditentukan oleh baris aktual. Sehingga huruf pertama dienkripsi tanpa pergeseran, huruf kedua dengan pergeseran ditentukan oleh baris kedua (jadi oleh satu posisi), huruf ketiga dengan pergeseran yang ditentukan oleh baris ketiga (jadi oleh dua posisi) dan seterusnya.

2.3 Penyimpanan *File Online*

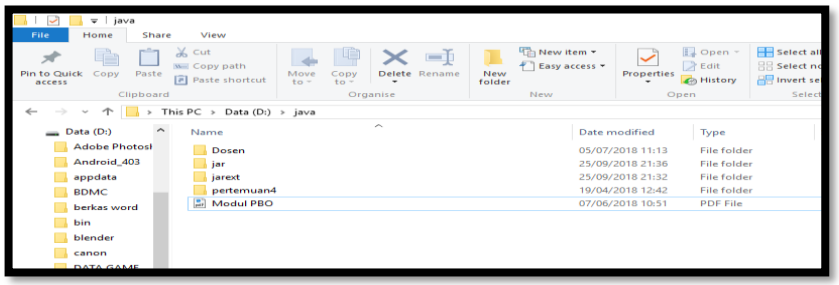
Penyimpanan file secara online memiliki banyak keuntungan salah satunya yaitu dapat dilihat melalui telepon selular, tablet, komputer yang terhubung ke *internet* dan dapat menyediakan *backup* sehingga tidak akan pernah kehilangan *file* apabila telepon selular hilang atau komputer rusak. Menggunakan penyimpanan *online* sangat mudah, namun menentukan layanan mana yang terbaik adalah lebih sulit.

3. HASIL DAN PEMBAHASAN

Prosedur yang dilakukan saat mengamankan file yaitu dengan memilih file yang belum dienkrip kemudian file tersebut dienkrip menggunkan Algoritma Trithemius sehingga file tersebut berhasil dienkrip atau diamankan. Setelah file tersebut berhasil dienkrip kemudian di upload sehingga file tersebut akan muncul atau tampil pada menu halaman awal aplikasi penyimpanan online yang sudah dihostingkan. Dan apabila ingin memulihkan *file* maka pilih File yang sudah berhasil dienkripsi yaitu pada halaman awal kemudian file tersebut didekripsi menggunakan Algoritma Trithemius sehingga akan mengembalikan *file* seperti semula.

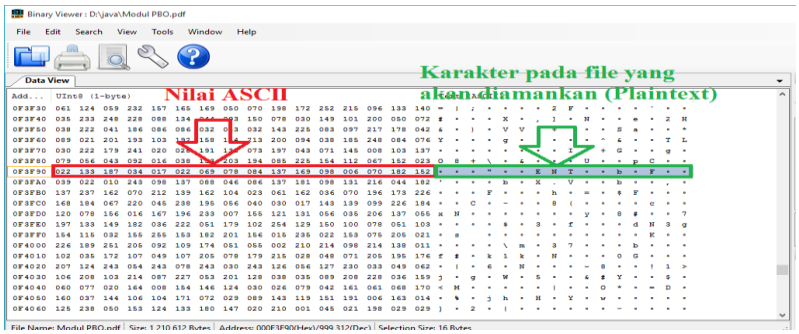
3.1 Penerapan Algoritma Trithemius

Penerapan algoritma merupakan tahapan terepenting dalam pengujian algoritma, karena dari proses tersebut dapat diketahui dari cara kerja dalam algoritma tersebut, dalam menyelesaikan suatu masalah. Sebagai pembuktian analisa maka penulis ingin melakukan pengamanan terhadap *file*. *File* yang akan diamankan adalah *file* berektensi PDF dengan nama *file* "Modul PBO" yang terletak pada direktori "D:\java" seperti yang dapat dilihat pada gambar 1. berikut ini.



Gambar 1. *File* yang akan diamankan

Setelah dipilih *file* yang akan diamankan, lalu *file* tersebut akan dienkripsi menggunakan Algoritma Trithemius. Untuk mengambil nilai ascii dari *file* yang akan diamankan tersebut maka digunakan *binary viewer*. Berikut adalah proses pengambilan nilai ascii menggunakan *binary viewer* dapat dilihat pada gambar 2.



Gambar 2. Nilai ASCII yang akan diamankan

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 3, Nomor 1, September 2021
e-ISSN 2685-998X
DOI 10.30865/json.v3i1.2630

Berdasarkan contoh diatas di dapatkan nilai dari aplikasi *binary viewer*, dan adapun karakter yang menjadi *plaintext* yaitu " …»" ENT‰ © b F ¶˜ " dengan nilai ascii : "022,133,187,034,017,022,069,078,084,137,169,098,006,070,182,152".

1. Proses Enkripsi

Langkah selanjutnya yaitu dengan merubah plaintext menjadi ciphertext menggunakan rumus berikut ini :

Enkripsi :
C = P + (Urutan Karakter – 1) Mod 255
Dekripsi :
P = C – (Urutan Karakter -1) Mod 255

Dimana :
C : *Ciphertext*
P : *Plaintext*

a. Karakter dengan kode ascii "022", maka :
C = 22 + (1 - 1) mod 255
= 22 mod 255
= 22 ( )
b. Karakter dengan kode ascii "133", maka :
C = 133 + (2 – 1) mod 255
= 134 mod 255
= 134 (†)
c. Karakter dengan kode ascii "187", maka :
C = 187 + (3 – 1) mod 255
= 189 mod 255
= 189 (½)
d. Karakter dengan kode ascii "034", maka :
C = 34+(4 – 1) mod 255
= 37 mod 255
= 37 (%)
e. Karakter dengan kode ascii "017", maka :
C = 17 + (5 – 1) mod 255
= 21 mod 255
= 21 ( )
f. Karakter dengan kode ascii "022", maka :
C = 22 + (6 – 1) mod 255
= 27 mod 255
= 27 ( )
g. Karakter dengan kode ascii "069", maka :
C = 69 + (7 – 1) mod 255
= 75 mod 255
= 75 (K)
h. Karakter dengan kode ascii "078", maka :
C = 78 + (8 – 1) mod 255
= 85 mod 255
= 85 (U)
i. Karakter dengan kode ascii "084", maka :
C = 84 + (9 – 1) mod 255
= 92 mod 255
= 92 (\ )
j. Karakter dengan kode ascii "137", maka :
C = 137 + (10 – 1) mod 255
= 146 mod 255
= 146 (')
k. Karakter dengan kode ascii "169", maka :
C = 169 + (11 – 1) mod 255
= 179 mod 255
= 179 (³)
l. Karakter dengan kode ascii "98", maka :
C = 98 + (12 – 1) mod 255
= 109 mod 255
= 109 (m)

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 3, Nomor 1, September 2021
e-ISSN 2685-998X
DOI 10.30865/json.v3i1.2630

m. Karakter dengan kode ascii “06”, maka :
C = 6 + (13 – 1) mod 255
= 18 mod 255
= 18 ( )
n. Karakter dengan kode ascii “70”, maka :
C = 70 + (14 – 1) mod 255
= 83 mod 255
= 83 (S)
o. Karakter dengan kode ascii “182”, maka :
C = 182 + (15 – 1) mod 255
= 196 mod 255
= 196 (Ä)
p. Karakter dengan kode ascii “152”, maka :
C = 152 + (16 – 1) mod 255
= 167 mod 255
= 167 (§)

Berdasarkan perhitungan diatas maka didapatkan cipherteks “†½%KU\’ ³mSÄ§”, dengan kode ascii yang bernilai “22,134,189,37,21,27,75,85, 92,146,179,109,18,83,196,167”.

2. Proses Dekripsi
a. Karakter dengan kode ascii “22”, maka :
P = 22 - (1 - 1) mod 255
= 22 mod 255
= 22 ( )
b. Karakter dengan kode ascii “134”, maka :
P = 134 - (2 – 1) mod 255
= 133 mod 255
= 133 (…)
c. Karakter dengan kode ascii “189”, maka :
P = 189 - (3 – 1) mod 255
= 187 mod 255
= 187 (»)
d. Karakter dengan kode ascii “37”, maka :
P = 37 - (4 – 1) mod 255
= 34 mod 255
= 34 (")
e. Karakter dengan kode ascii “21”, maka :
P = 21 - (5 – 1) mod 255
= 17 mod 255
= 17 ()
f. Karakter dengan kode ascii “27”, maka :
P = 27 - (6 – 1) mod 255
= 22 mod 255
= 22 ( )
g. Karakter dengan kode ascii “75”, maka :
P = 75 - (7 – 1) mod 255
= 69 mod 255
= 69 (E)
h. Karakter dengan kode ascii “85”, maka :
P = 85 - (8 – 1) mod 255
= 78 mod 255
= 78 (N)
i. Karakter dengan kode ascii “92”, maka :
P = 92 - (9 – 1) mod 255
= 84 mod 255
= 84 (T)
j. Karakter dengan kode ascii “146”, maka :
P = 146 - (10 – 1) mod 255
= 137 mod 255
= 137 (‰)
k. Karakter dengan kode ascii “179”, maka :
P = 179 - (11 – 1) mod 255
= 169 mod 255

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 3, Nomor 1, September 2021
e-ISSN 2685-998X
DOI 10.30865/json.v3i1.2630

= 169 (©)

l. Karakter dengan kode ascii “109”, maka :
P = 109 - (12 – 1) mod 255
= 98 mod 255
= 98 (b)

m. Karakter dengan kode ascii “18”, maka :
P = 18 - (13 – 1) mod 255
= 6 mod 255
= 6 ( )

n. Karakter dengan kode ascii “83”, maka :
P = 83 - (14 – 1) mod 255
= 70 mod 255
= 70 (F)

o. Karakter dengan kode ascii “196”, maka :
P = 196 - (15 – 1) mod 255
= mod 255
= 182 (¶)

p. Karakter dengan kode ascii “167”, maka :
P = 167 - (16 – 1) mod 255
= 153 mod 255
= 152 (˜)

Berdasarkan hasil dari proses dekripsi diatas, maka cipherteks akan kembali ke plainteks yaitu “ …»" ENT‰ © b F ¶˜ ”.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, maka hasil akhir dari penelitian tersebut dapat diambil beberapa kesimpulan dari pembahasan sebelumnya, adapun kesimpualan Prosedur enkripsi dan dekripsi dengan menggunakan Algoritma Trithemius telah berhasil melakukan pengamanan *file* sehingga proses enkripsi dapat berjalan sesuai dengan yang diharapkan. Algoritma Trithemius dapat diterapkan pada aplikasi penyimpanan *file* secara *online* telah membuktikan bahwa tidak hanya tipe file .pdf yang dapat diamankan, namun tipe *file* yang berekstensi .word juga dapat diamankan bahkan tipe *file* lainnnya juga dapat diamankan pada aplikasi. Aplikasi pengamanan *file* telah selesai dirancang dengan menggunakan apliksai *Adobe Dreamweaver CS6* dengan menggunakan bahsa pemograman PHP dan menerapkan Algoritma Trithemius sehingga memudahkan penulis dalam mengamankan file.

REFERENCES

[1] A. Prayitno and N. Nurdin, “ANALISA DAN IMPLEMENTASI KRIPTOGRAFI PADA PESAN RAHASIA,” vol. 3, no. 1, pp. 1–11, 2017.
[2] Y. Prihantono and G. Bagi, “PENGEMBANGAN APLIKASI PENGAMANAN FILE SEBAGAI SOLUSI KEAMANAN DATA PADA SMARTPHONE BERBASIS,” pp. 2–8, 2016.
[3] E. Setyaningsih, *Kriptografi & Implementasinya menggunakan MATLAB*. Yogyakarta: Penerbit ANDI, 2015.
[4] D. Salomon, *Data Privacy and Security*. USA, 2003.
[5] R. A. S and M. Shalahuddin, *REKAYASA PERANGKAT LUNAK*. Bandung: informatika, 2016.
[6] N. Firly, *Create Your Own android Application*. Bogor: PT Elex Media Komputindo, 2018.
[7] S. K. Alfa Satyaputa, M.sc EvaMaulina Aritonang, *Java for beginners with eclipse 4.2 juno*. Jakarta, 2012.