Jurnal Pendidikan Sains dan Komputer

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1378

Algoritma ADFGVX Product Transposition Cipher pada Pengenkripsian Pesan Text

Bela Dina[1], Dadang Iskandar Mulyana[2], Julinar Sari Hutagalung[3]
[1-3] Fasikom, Sistem Informasi, Stikom CKI, Jakarta, Indonesia
[1)]beladina97@gmail.com, [2)]mahvin2012@gmail.com, [3)]julinarhutagalung99@gmail.com

open access

***Penulis Korespondensi**

Histori Artikel:
Submit: 2022-02-15
Diterima: 2022-03-01
Dipublikasikan: 2022-03-13

Kata Kunci:
Algoritma ADFGVX; Enkripsi; Dekripsi; Plain Text; Cipher Text

Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

ABSTRAK

Keamanan informasi data digital menjadi hal yang penting dan sangat diperlukan untuk menjaga data yang penting dan rahasia. Salah satu solusi yang ditawarkan untuk mengamankan data dengan sebuah cara menyandikan data atau disebut juga dengan ciphering. Dalam kriptografi terdapat beberapa metode yang sangat penting dalam menjaga kerahasiaan suatu data yakni enkripsi dan dekripsi. Algoritma ADFGVX Product Cipher dibuat karena merupakan salah satu algoritma yang memiliki sandi morse yang jelas. Algoritma ini akan menciptakan fungsi enkripsi kompleks seperti cara menggabungkan beberapa operasi enkripsi dasar sederhana yang saling melengkapi sehingga melibatkan operasi bolak-balik yang berulang yaitu subtitusi dan permutasi.

Algoritma Row Transposition dipilih karena cipher transposisi dimana plainteks dituliskan per kolom sesuai panjang kunci dan dibaca berdasarkan urutan indeks huruf tersebut per kolom.

LATAR BELAKANG

Keamanan merupakan masalah besar dan mengamankan data yang penting sangat penting, sehingga data tersebut tidak dapat disadap atau disalahgunakan untuk tujuan ilegal sehingga merugikan pihak lain. [1]

Kriptografi merupakan salah satu metode pengamanan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data, serta keaslian pengiriman. Metode ini bertujuan untuk informasi yang bersifat rahasia yang dikirim melalui telekomunikasi umum tidak dapat diketahui atau dimanfaatkan dengan orang yang tidak berkepentingan atau yang tidak berhak menerimanya. Metode kriptografi yang dapat digunakan untuk mengamankan data dll.[2]

Kriptografi bisa diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, autentikasi data. karena tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi.[3]

Enkripsi adalah metode yang digunakan untuk mengubah informasi menjadi kode rahasia yang menyembunyikan makna sebenarnya dari informasi tersebut. Ilmu enkripsi dan dekripsi informasi disebut juga kriptografi. Dalam komputasi, data yang tidak terenkripsi juga dikenal sebagai plaintext, dan data terenkripsi disebut ciphertext. Rumus yang digunakan untuk menyandikan dan mendekode pesan disebut algoritma enkripsi atau sandi. Agar efektif, sandi 22 menyertakan variabel sebagai bagian dari algoritma.[4]

Dekripsi adalah proses mengambil teks yang disandikan atau dienkripsi atau data lain dan mengubahnya kembali menjadi teks yang dapat Anda baca dan pahami oleh komputer. Istilah ini dapat digunakan untuk menggambarkan metode tidak mengenkripsi data secara manual atau tidak mengenkripsi

Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1378

data menggunakan kode atau kunci yang tepat. Data dapat dienkripsi untuk menyulitkan seseorang untuk mencuri informasi.[5]

STUDI LITERATUR

Plain Text adalah teks yang diencode dalam sebuah format ASCII. Plain text tidak memiliki format, informasi struktur seperti ukuran dan tipe font, warna, ataupun layout. Plain text biasanya digunakan antar-komputer yang tidak memiliki kesepakatan untuk saling bertukar informasi format dan layout teks.[6]

Ciphertext adalah bentuk setelah pesan dalam plaintext telah diubah bentuknya menjadi lebih aman dan tidak dapat dibaca. Proses mengubah plaintext menjadi ciphertext disebut encryption (enciphering),juga proses membalikkannya kembali disebut decryption (deciphering).[7]

Setiap metode memiliki kelebihan dan kekurangannya masing-masing. Namun, yang jadi permasalahan dalam memilih metode kriptografi yang cocok adalah bagaimana mengetahui dan memahami cara kerja dari metode kriptografi tersebut. Dalam proses komunikasi data, walaupun data sudah dienkripsi kemungkinan data tersebut dapat diketahui oleh orang lain. Salah satu kemungkinan tersebut adalah orang menyadap media komunikasi yang dituliskan oleh kedua orang yang sedang berkomunikasi. ADFGVX adalah cryptanalysed dengan Bahasa Perancis Tentera Leftenan Georges Painvin, dan cipher itu rosak pada awal Jun 1918. Karya ini sangat sulit oleh standard kriptografi klasik, dan akhirnya Painvin jatuh sakit secara fizikal selama ini. Kaedah pekerjaannya bergantung pada mencari pesan dengan permulaan yang stereotaip, yang akan memecahkannya dan kemudian membentuk gambar yang serupa dalam posisi di ciphertext yang sesuai dengan tajuk lajur dalam tabel transposisi. (Analisis statistik yang cukup diperlukan setelah Langkahnya dicapai, semuanya dilakukan dengan tangan.) Oleh itu, ia hanya berkesan pada masa lalu lintas yang sangat tinggi, tetapi itu juga ketika mesej yang paling penting dihantar.[8]

Studi Literatur Pada tahap ini dilakukan studi literatur dengan mempelajari kriptografi, algoritma ADFGVX cipher, algoritma knapsack serta bahasa pemrograman C# melalui peninjauan terhadap buku, artikel, jurnal, maupun hasil penelitian Analisis dan Perancangan Tahapan ini digunakan untuk mengolah data yang didapatkan dari studi literatur yang kemudian dilakukan analisis dan perancangan dengan menggunakan algoritma ADFGVX cipher dan knapsack sehingga menjadi sebuah aplikasi yang terstruktur, jelas, dan berjalan dengan baik. Proses ini meliputi pembuatan algoritma program, flowchart algoritma, flowchart system, use case scenario, perancangan aplikasi, dan pembuatan user interface. [9]

METODE

Metodologi Penelitian Tahapan yang dilakukan pada penelitian ini adalah studi Literatur Pada tahap ini dilakukan studi literatur dengan mempelajari kriptografi, algoritma ADFGVX cipher, algoritma knapsack serta bahasa pemrograman C# melalui peninjauan terhadap buku, artikel, jurnal, maupun hasil penelitian

Analisis dan Perancangan Tahapan ini digunakan untuk mengolah data yang didapatkan dari studi literatur yang kemudian dilakukan analisis dan perancangan dengan menggunakan algoritma ADFGVX cipher dan knapsack sehingga menjadi sebuah aplikasi yang terstruktur, jelas, dan berjalan dengan baik. Proses ini meliputi pembuatan algoritma program, flowchart algoritma, flowchart system, use case scenario, perancangan aplikasi, dan pembuatan user interface. [9]

Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

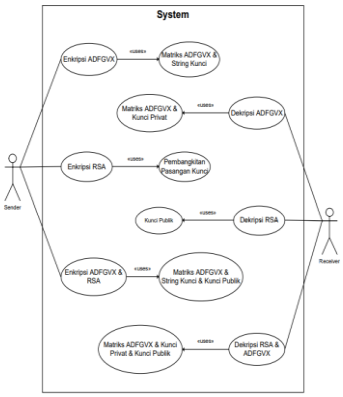
Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1378

Tahapan Penelitian

Metode kriptografi ADFGVX yang digunakan oleh tentara Jerman pada Perang Dunia I adalah merupakan salah satu algoritma yang paling dikenal dalam sejarah kriptografi. Algoritma ini ditemukan dengan seorang petugas radio tentara Jerman yang bernama Fritz Nebel (1891 - 1967)[6]. Algoritma ini pertama kali pada tanggal 5 Maret 1918 ketika pihak Jerman menggunakannya dalam sebuah transmisi pesan nirkabel di medan perang di bagian barat Eropa. Disebutkan algoritma ADFGVX karena chiperteks hasil enkripsi pesan tentara Jerman hanya mengandung enam karakter alphabet. awalnya algoritma ini hanya menggunakan 5 karakter saja. Tetapi pada perkembangannya ditambahkan karakter huruf X agar algoritma ini dapat menangani 26 huruf alphabet dan 10 angka. Huruf-huruf A, D, F, G, V, dan X sendiri dipilih karena representasi huruf ini tersebut dalam sandi morse sangat berbeda dan juga karenanya memperkecil kemungkinan terjadinya kesalahan dalam penerimaan di kotak pesan. Algoritma ADFGVX cipher menggunakan sebuah tabel 6 x 6 yang berisi 26 huruf dan 10 angka (0-9). Enkripsinya terdapat dua proses, yaitu proses substitusi dan proses transposisi. Selain itu Setiap proses tersebut membutuhkan sebuah kunci.[10]

Use-Case Diagram

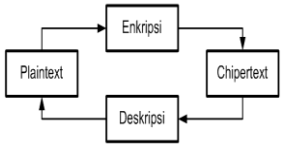
Untuk menganalisa komponen-komponen yang berperan dalam sistem yang dirancang, penulis menggunakan use-case diagram agar proses penganalisaan komponen dapat dilakukan dengan mudah. Use-case diagram sistem pada aplikasi yang dirancang dapat dilihat pada Gambar 1.[11]



Gambar 1. Use-Case Diagram Pada Sistem

HASIL

Skema proses enkripsi dan dekripsi secara sederhana dapat dilihat pada gambar dibawah ini :



Proses Enkripsi

Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Jurnal Pendidikan Sains dan Komputer
Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1378

Enkripsi merupakan sebuah proses dimana data teks asli diubah menjadi data pesan secrot. Sebelum melakukan enkripsi, data yang akan dienkripsi (plainteks) diatur terlebih dahulu sebagai berikut :

1. Semua spasi dan karakter yang bukan alphabet dan angka harus dihapus dari plainteks

2. Pesan yang akan dienkripsi ditulis dalam kedua berurut(bigram)

3. Kunci dimasukkan ke tabel ukuran 6 x 6

Contoh Kasus:

Pesan = THIS IS A SECRET

Kunci 1= C3A1LI9F6ORNB2D4E5G7H8J0KMPQSTUV WXYZ

Kunci 2=APOLLO

Berikut ada langkah-langkah dalam mengenkripsi sebuah pesan plainteks dan menggunakan algoritma ADFGVX Cipher :

1. Tentukan kunci awal yang terdiri dari huruf dan angka, misalkan

   “C3A1LI9F6ORNB2D4E5G7H8J0KMPQS TUVWXYZ”. Jika ada huruf berulang-ulang maka cukup satu huruf yang muncul pertama yang dituliskan.

2. 2. Buatlah sebuah tabel 6 x 6 dan isi dengan kunci pertama, kemudian huruf-huruf berurutan yang belum muncul, dan selanjutnya angka-angka berurutan yang belum muncul. Tabel berikut ini merepresentasikan tabel yang harus terbentuk dengan kunci “C3A1LI9F6ORNB2D4E5G7H8J0KMPQS TUVWXYZ”.

Tabel 1 Tabel Kunci 1

	A	D	F	G	V	X
A	C	3	A	1	L	I
D	9	F	6	O	R	N
F	B	2	D	4	E	5
G	G	7	H	8	J	0
V	K	M	P	Q	S	T
X	U	V	W	X	Y	Z

Penyelesaian : THIS IS A SECRET Enkripsikan T jadi VX ditunjukkan pada papan kunci dibawah ini

Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1378

Tabel 2 Enkripsi T

	A	D	F	G	V	X
A	C	3	A	1	L	I
D	9	F	6	O	R	N
F	B	2	D	4	E	5
G	G	7	H	8	J	0
V	K	M	P	Q	S	T
X	U	V	W	X	Y	Z

Proses Dekripsi

Berikut ini adalah langkah-langkah dalam mendekripsi sebuah chipertext menjadi plainteks dengan menggunakan metode ADFGVX yaitu =

1. Sebelumnya kita wajib mengetahui kunci 2 dari proses ini. Seterusnya bagikan jumlah karakter hasil enkripsi dengan panjang kunci ke 2 dimana panjang chipertext=36 dan panjang kunci=6 sehingga diperoleh banyak karakter per kolom dengan 36/6=6 karakter. Gambarkan hasilnya kedalam kotak kunci sebagai berikut :

2. Susunlah kembali hasil dari langkah 1 sesuai kunci ke 2 yaitu “kunci” . Untuk menemukan hasil dari pengurutan ALLOOP menjadi APOLLO maka harus dilakukan proses perulanangan sebanyak n! dimana

: n = panjang kunci sehingga bisa mendapatkan kunci tersebut maka dibutuhkan sebanyak 6! Proses pencarian yaitu sebanyak 720 kali kemungkinan diantaranya :

Allop Aollp

Allpo Aollp

Alplo Aopll

Alopl Aolpl

Allop Aoplp

Sampai akhirnya diperoleh hasil APOLLO. Adapun proses percobaan tersebut sehingga diperoleh hasil berikut ini:

A	P	O	L	L	O
V	X	G	F	A	X
V	V	A	X	V	V
A	F	V	V	F	V
A	A	D	V	F	V
V	X	X	X	X	X
X	X	X	X	X	X

3. Susun kembali huruf yang ada di tabel kunci dengan bentuk bigram yaitu berpasangan, sehingga menjadi VX GF AX VV AX VV AF VV FV AA DV FV VX XX XX XX XX XX 4. Selanjutnya cari padanan dari

Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1378

abjad berpasangan diatas yang diperoleh dari kunci 1

	A	D	F	G	V	X
A	C	3	A	1	L	I
D	9	F	6	O	R	N
F	B	2	D	4	E	5
G	G	7	H	8	J	0
V	K	M	P	Q	S	T
X	U	V	W	X	Y	Z

Alur proses enkripsidengan menggunakan algoritma ADFGVX Cipher pada aplikasi yang dirancang dapat dijelaskan pada flowchart seperti pada Gambar 4

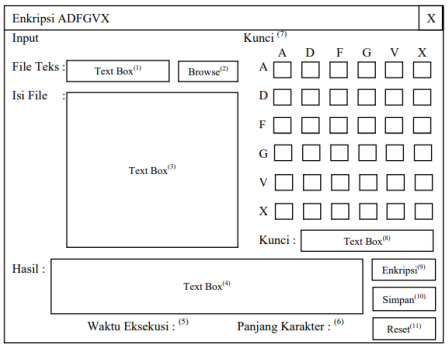
A	L	L	O	O	P
V	F	A	G	X	X
V	X	V	A	V	V
A	V	F	V	V	F
A	V	F	D	V	A
V	X	X	X	X	X
X	X	X	X	X	X

Rancangan Halaman Enkripsi ADFGVX

Rancangan halaman menu Enkripsi ADFGVX berfungsi untuk melakukan proses enkripsi pada file teks dan dokumen menggunakan algoritma ADFGVX. Tampilan halaman menu Enkripsi dapat dilihat pada Gambar 4.

Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1378



Gambar 4. Rancangan Halaman Enkripsi ADFGVX

Keterangan:

1. TextBox berfungsi untuk menampilkan lokasi file.

2. CommandButton yang berfungsi untuk membuat lokasi dan nama file.

3. TextBoxyang berfungsi untuk menampilkan isi file.

4. TextBox berfungsi untuk menampilkan hasil enkripsi (ciphertext).

5. Label yang berfungsi untuk menampilkan waktu eksekusi proses enkripsi.

6. Label yang berfungsi untuk menampilkan panjang karakter file hasil enkripsi.

7. Sekumpulan TextBox berfungsi untuk memasukkan 26 karakter huruf dan angka yang akan digunakan sebagai kunci.

8. TextBoxSecurity of digital data information is important and very necessary to keep important and confidential data. One of the solutions offered to secure data is by encoding the data or also known as ciphering. In cryptography there are several methods that are very important in maintaining the confidentiality of data, namely encryption and decryption. The ADFGVX Product Cipher algorithm was created because it is one of the algorithms that has a clear Morse code. This algorithm will create complex encryption functions such as how to combine several simple basic encryption operations that complement each other so that it involves repeated back and forth operations, namely substitution and permutation.

Row Transposition Algorithm was chosen because it is a transposition cipher where the plaintext is written per column according to the key length and is read based on the index order of the letters per column. berfungsi untuk memasukkan kunci yang sangat privat.

9. CommandButton berfungsi untuk melakukan proses enkripsi pada file.

10. CommandButton yang berfungsi untuk melakukan proses penyimpanan file hasil enkripsi. 11. CommandButton yang berfungsi untuk mengembalikan sistem ke kondisi semula.

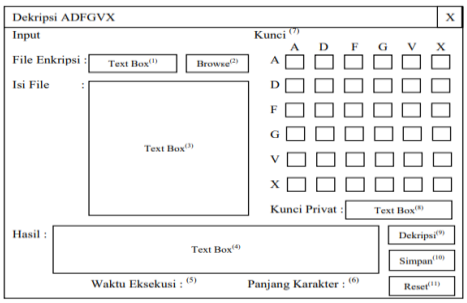
PEMBAHASAN

Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1378

Rancangan Halaman Dekripsi ADFGVX

Rancangan di menu Dekripsi ADFGVX berfungsi untuk melakukan proses dekripsi pada file ciphertext menggunakan algoritma ADFGVX. Tampilan halaman menu Dekripsi dapat dilihat pada Gambar 5



Gambar 5. Rancangan Halaman Dekripsi ADFGVX

Keterangan:

1. TextBox yang berfungsi untuk menampilkan lokasi file.

2. CommandButton berfungsi untuk memasukkan lokasi dan nama file.

3. TextBox berfungsi untuk menampilkan isi file.

4. TextBoxyang berfungsi untuk menampilkan hasil dekripsi.

5. Label yang berfungsi untuk menampilkan waktu eksekusi proses dekripsi.

6. Label berfungsi untuk menampilkan panjang karakter file hasil dekripsi.

7. TextBoxyang berfungsi untuk memasukkan 26 karakter angka dan huruf yang akan digunakan sebagai kunci.

8. TextBoxyang berfungsi untuk memasukkan kunci privat.

9. CommandButton yang berfungsi untuk melakukan proses dekripsi file

10. CommandButton yang berfungsi untuk melakukan proses penyimpanan file hasil dekripsi. 11. CommandButton yang berfungsi untuk mengembalikan sistem ke kondisi semula.

Pengujian EnkripsiADFGVX Cipher

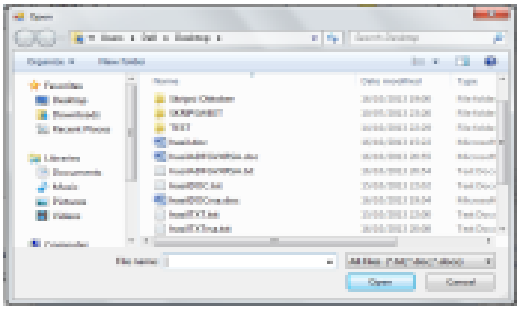
Untuk melakukan enkripsi file melalui aplikasi yang dirancang dapat dilakukan dengan cara memulai aplikasi kemudian ketika tampilan aplikasi telah muncul seperti Gambar 4.1, lakukan langkah-langkah sebagai berikut: 1. Menekan tombol Browsemaka akan muncul pop-up window Open yang akan menampilkan jendela penyimpanan file. Pop-up Window Open dapat dilihat pada dibawah ini4.20.

1. Menekan tombol Browsemaka akan muncul pop-up window Open yang akan menampilkan jendela

Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1378

penyimpanan file. Pop-up Window Open dapat dilihat pada Gambar4.20



Gambar 4.20Pop-up Window Open

2. Kemudian akan muncul isi dari file teks atau dokumen yang telah dipilih. Setelah itu user menginputkan kunci yang terdiri dari 26 karakter huruf dan 10 karakter angka pada tabel 6x6 yang telah disediakan.Dan juga user menginputkan kunci privat yang akan digunakan untuk enkripsi. Tampilan input karakter huruf dan angka serta kunci privat bisa dilihat pada Gambar 4.21



Gambar 4.21 Tampilan Input Karakter Huruf dan Angka serta Kunci Privat

3. Proses enkripsi dapat dilakukan dengan cara mengeksekusi tombol Enkripsi. Setelah proses enkripsi selesai dilakukan maka akan muncul file ciphertext hasil enkripsi dan menampilkan informasi tentang enkripsi seperti waktu eksekusi proses enkripsi dan panjang karakter file ciphertext hasil enkripsi. Tampilan proses enkripsi file menggunakan ADFGVX Cipher dapat dilihat pada berikut ini 4.22.



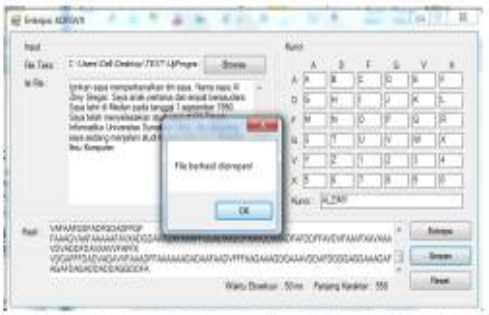
Gambar 4.22 Proses Enkripsi File Menggunakan ADFGVX *Cipher*

Untuk melakukan proses penyimpanan file dapat dilakukan dengan cara mengeksekusi tombol Simpan. Kemudian ketikkan nama file yang akan disimpan. Jika proses penyimpanan berhasil, maka akan muncul

Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1378

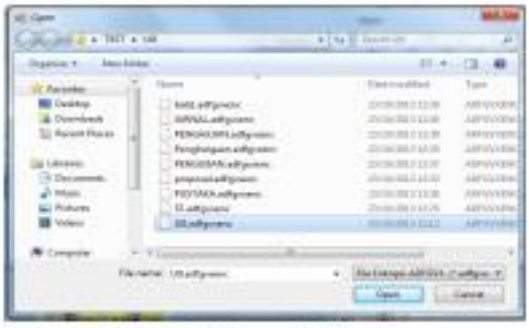
tampilan seperti pada Gambar 4.12.



Gambar 4.23 Proses Penyimpanan File Enkripsi ADFGVX *Cipher*

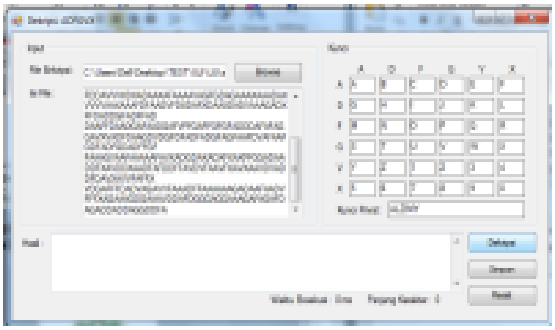
Pengujian DekripsiADFGVX Cipher

Untuk melakukan dekripsi pada file hasil enkripsi dapat dilakukan dengan cara memulai aplikasi kemudian ketika tampilan aplikasi telah muncul seperti Gambar diatas 4.1, lakukan dengan Langkah sebagai berikut:
1. Menekan tombol Browse akan muncul pop-up window Open yang akan menampilkan jendela penyimpanan file. Pop-up Window Open bisa dilihat pada Gambar4.24



Gambar 4.24*Pop-up Window Open*

2. Kemudian akan muncul isi dari file hasil enkripsi (ciphertext) yang telah dipilih. Setelah itu user menginputkan kunci yang terdiri dari 26 karakter huruf dan 10 karakter angka pada tabel 6x6 yang telah disediakan.Dan juga user menginputkan kunci privat. Tampilan input karakter huruf ,angka serta kunci privatdapat dilihat pada Gambar 4.25.



Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1378

Gambar 4.25 Tampilan Input Karakter Huruf dan Angka serta Kunci Privat Proses Dekripsi

3. Proses dekripsi bisa dilakukan dengan cara mengeksekusi tombol Dekripsi. Setelah proses dekripsi selesai dilakukan maka muncul file aslihasil dekripsi dan menampilkan informasi-informasi tentang dekripsi seperti waktu eksekusi proses dekripsi dan panjang karakter file baru. Tampilan proses dekripsi file menggunakan ADFGVX Cipher dapat dilihat pada Gambar 4.26.



Gambar 4.26 Proses Dekripsi File Menggunakan ADFGVX *Cipher*

KESIMPULAN

Berdasarkan hasil pengujian dan analisis terhadap Algoritma ADFGVX, dapat diambil beberapa kesimpulan sebagai berikut:

1. ADFGVX dengan papan kunci berbentuk bujursangkar dapat menyandikan pesan sehingga hanya pihak yang berhak saja yang dapat melihat isi pesan.
2. ADFGVX dengan menggunakan papan kunci adalah solusi yang lebih baik dalam mengatasi masalah keamanan dan kerahasian data teks.
3. Proses enkripsi dan dekripsi harus dilakukan dengan menggunakan papan kunci yang sama untuk mendapatkan isi arsip yang asal.

UCAPAN TERIMAKASIH *(PILIHAN)*

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.

REFERENSI

[1] "Perbandingan Algoritma AES (Advanced Encryption Standard) dan 3DES(Triple Data Encryption Algorithm) Menggunakan Manajemen Kunci."

[2] L. Benny, "ANALISIS DAN PERANCANGAN APLIKASI KRIPTOGRAFI KEAMANAN FILE BERBASIS TEKS DENGAN MENGGUNAKAN METODE RSA," *Riset dan E-Jurnal Manajemen Informatika Komputer*, vol. 1, no. 2, 2017.

[3] P. Widodo, D. Gunawan, P. Peperangan Asimetris, F. Strategi Pertahanan, and U. Pertahanan,

Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1378

"EFEKTIVITAS KEAMANAN INFORMASI DALAM MENGHADAPI ANCAMAN SOCIAL ENGINEERING EFFECTIVENESS OF INFORMATION SECURITY THREATS FACING SOCIAL ENGINEERING." [Online]. Available: http://fahmirahmatazis.co.id/2015/09/cybercrime-

[4] H. Adiyasa and S. Adhy, "IMPLEMENTASI ALGORITMA KRIPTOGRAFI DENGAN S-BOX DINAMIS BERGANTUNG PADA KUNCI UTAMA BERBASIS ADVANCED ENCRYPTION STANDARD (AES)," 2014.

[5] "Implementasi Kriptografi Algoritma AES Serta Algoritma Kompresi Huffman Dengan Menggunakan Pemograman PHP".

[6] S. Anwar, I. Nugroho, and A. Ahmadi, "Implementasi Kriptografi Dengan Enkripsi Shift Vigenere Chiper Serta Checksum Menggunakan CRC32 Pada Data Text," *Jurnal Sistem Informasi*, vol. 2, 2015.

[7] G. Gumira PUK and A. Erlanshari, "IMPLEMENTASI METODE ADVANCED ENCRYPTION STANDARD (AES) DAN MESSAGE DIGEST 5 (MD5) PADA ENKRIPSI DOKUMEN (STUDI KASUS LPSE UNIB)," *Jurnal Rekursif*, vol. 4, no. 3, 2016.

[8] D. Virgian and S. Y. Sakti, "PENERAPAN STEGANOGRAFI METODE END OF FILE (EOF) DAN ENKRIPSI METODE DATA ENCRYPTION STANDARD (DES) PADA APLIKASI PENGAMANAN DATA GAMBAR BERBASIS JAVA PROGRAMMING," 2014. [Online]. Available: https://www.researchgate.net/publication/273145116

[9] R. Novita Sari, I. Lazuly, K. Kunci, and M. Hellman, "Implementasi Algoritma Merkle Hellman Dalam Mengamankan Pesan Teks Implementation of The Merkel Hellman Algortihm in Securing Text Message."

[10] "Enkripsi Dekripsi Algoritma Elgamal Pada Pengiriman Email : ENDIMA", doi: 10.13140/RG.2.2.36509.33764.

[11] A. Fauzi and Y. Maulita, "ANALISIS SUPER ENKRIPSI ALGORITMA ONE TIME PAD DAN ALGORITMA ELGAMAL PADA KEAMANAN PESAN."

Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).