Journal of Information System and Technology, Vol.05 No. 03, Des 2024, pp. 31-36
ISSN : 2775-0272
DOI : 10.37253/joint.v5i3.10009

Contents list available at https://journal.uib.ac.id/
JOINT
(Journal of Information System and Technology)
journal homepage: https://journal.uib.ac.id/index.php/joint/

Penerapan Kriptografi untuk Enkripsi dan Dekripsi *Text* dengan Algoritma Subtitusi *Chipper*

Basorudin[1], Muhammad Thoriq[2], Muhammad Romi Nasution[3], Satria Riki Mustafa[4], Erni Rouza[5]
1,4,5Teknik Informatka, Fakultas Ilmu Komputer, Universitas Pasir Pengaraian
3Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pasir Pengaraian
2Informatika, Universitas Adzkia
E-mail: basorudin09@gmail.com[1], thoriq.if@adzkia.ac.id[2], m.romi.nst@upp.ac.id[3], satriarikimustafa@gmail.com[4], ernirouzait@gmail.com[5]

Abstrak

Kriptografi adalah bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi dan dekripsi. Teknik ini untuk mengkonversi data ke bentuk kode-kode tertentu agar informasi tidak dapat terbaca oleh siapapun, kecuali pihak yang berhak. Salah satu metode kriptografi yang biasa digunakan adalah algoritma simetris yang menggunakan kunci yang sama saat melakukan enkripsi dan dekripsi, sehingga informasi sulit dipahami maknanya. Tujuan dilakukannya enkripsi dan enkripsi data atau *text* ini adalah agar data yang dimiliki lebih aman dari serangan orang-orang yang tidak bertanggung jawab. Perangkat lunak dibangun dengan bantuan aplikasi Visual Basic. Setelah diimplementasikan proses dekripsi dan enkripsi *text* dengan algoritma Subtitusi *Chipper* dengan *Plaintext* INFORMATIKA menggunakan aplikasi yang telah dirancang dan dibuat, kemudian telah dilakukan pengujian dengan Microsoft Excel telah menghasilkan hasil *Chiphertext* yang sama yaitu dengan hasil SXPYBWKDSUK. Maka, dapat disimpulkan bahwa dekripsi dan enkripsi *text* dengan algoritma Subtitusi *Chipper* telah berhasil dilakukan dengan hasil valid atau sesuai dengan yang diharapkan.

Katakunci: kriptografi, enkripsi, dekripsi, *plaintext*, *chippertext*

I. PENDAHULUAN

Kebutuhan masyarakat akan keamanan informasi dengan adanya teknologi informasi, data-data informasi rahasia yang seharusnya tidak boleh diketahui orang lain kecuali pemilik informasinya sangat mungkin terjadi, karena hal tersebut termasuk dalam teknologi informasi dalam hal keamanan informasi. Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan, data, atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna [1].

Kriptografi berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi, tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi [2].

Banyak cara dapat dilakukan untuk menyembunyikan data atau pesan yang akan dikirim. Salah satunya menggunakan kriptografi. Kriptografi berfungsi untuk menyamarkan pesan menjadi pesan yang tersandi. Adapun algoritma kriptografi yang bisa menyamarkan pesan adalah algoritma *Caesar Cipher* dan Transposisi *Cipher*. Algoritma *Caesar Cipher* adalah algoritma penyandian data paling sederhana dengan cara mengenkripsi dan mendekripsi data dengan menggunakan pergeseran sebanyak. Algoritma Tranposisi *Chiper* adalah algoritma penyandian teks pesan yang akan disandikan dengan cara diubah posisinya [3].

Dalam penelitian ini, akan menerapkan kriptografi untuk enkripsi dan dekripsi *text* dengan algoritma Subtitusi *Cipher*, karena keamanan data suatu hal yang sangat diperlukan diera digital seperti saat ini. Dalam penelitan ini, nantinya enkripsi dan dekripsi *text* akan dibangun dengan mengguakan aplikasi Visual Basic dan pengujiannya dilakukan dengan bantuan Microsoft Excel. Pengujian dikatakan berhasil atau valid ketika hasil yang ada pada aplikasi Visual Basic sama dengan hasil yang ada pada Microsoft Excel.

Penelitian terkait yang diangkat oleh (Muhammad Zulham, dkk., 2014), dengan judul "Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi Rc6 Berbasis Android", pada penelitian ini mendapatkan hasil bahwa pesan dapat disandikan sehingga keamanan isi pesan sangat terjaga dalam kerahasiaan data selanjutnya. Aplikasi ini mampu mengirim dan menerima pesan melalui email yang berjalan di sistem operasi Android dengan menggunakan aplikasi DroidRC6 [4].

Proses keamanan dengan melakukan pergantian karakter yang terdapat pada sebuah teks menjadi karakter yang lain. Karakter yang diganti dapat berupa angka maupun huruf. Konsep kerja dari Substitusi *Cipher* ditunjukan pada Gambar 2 sebagai contoh kerja Substitusi *Cipher* dengan pergeseran [5].

Penelitian terdahulu yang diangkat oleh (Faturungi Muharram, dkk., 2018) dengan judul "Analisis Algoritma pada Proses Enkripsi dan Dekripsi *File* Menggunakan *Advanced Encryption Standard* (AES)". Dari hasil uji coba pada proses enkripsi dan dekripsi, maka dapat disimpulkan bahwa *file* yang melalui uji coba dekripsi akan berubah bentuk menjadi *file* yang tak bisa dibaca. *File* dapat kembali ke bentuk asli jika melalui proses dekripsi dengan menggunakan kunci yang sama saat enkripsi. Waktu proses hasil enkripsi-dekripsi data dapat dipengaruhi oleh besar ukuran data yang akan di uji [6].

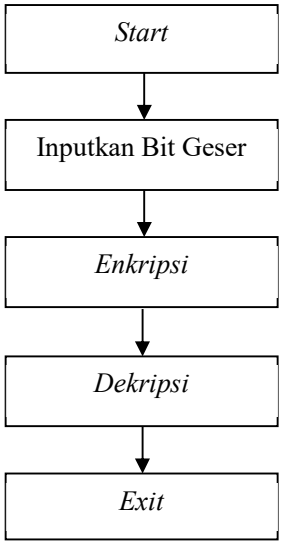
Tabel 1. Proses Uji Algoritma pada *File* dan *Testing*

No	Nama File	Kata Kunci	Ukuran File	Waktu Enkripsi	Waktu Dekripsi
1	Haha.png	123456	468,08 Kb	00:00:43	00:00:47
2	Tes2.jpg	111111	78,93 Kb	00:00:2	00:00:3
3	Tes3.jpg	111112	12,37 Kb	00:00:1	00:00:1

Perbedaan penelitian ini dengan penelitan yang akan diangkat adalah menggunakan algoritma Subtitusi *Cipher* dengan bit geser menggunakan Visual Basic dan dilakukan pengujian dengan Microsoft Excel. Misalnya, *plaintext* dengan nama Informatika dengan Bit Geser 10 akan dilakukan proses acak (*Chipertext*) dengan aplikasi Visual Basic yang akan dibangun dan diuji dengan Microsoft Excel.

II. METODE PENELITIAN

Dalam penelitian ini, metode keamanan data yang akan digunakan yaitu dengan algoritma Subtitusi *Cipher*.



Gambar. 1 Metodologi Penelitian

Data yang dugunakan adalah berupa kata atau kalimat, kemudian kata atau kalimat tersebut akan di enkripsi dengan dengan Bit geser tertentu, dan setelah dienkrip maka kalimat tersebut menjadi data acak yang tidak dapat dipahami atau data yang tidak memiliki makna. Kemudian, data yang sudah dienkripsi dapat didekripsi kembali atau dijadikan data asli yang dapat dibaca dan memiliki makna.

III. HASIL DAN PEMBAHASAN

A. Kriptografi

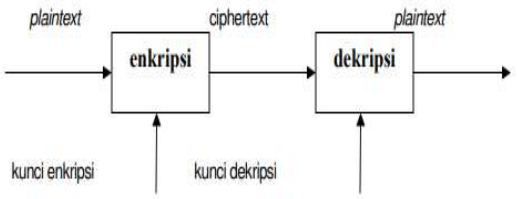
Kriptografi adalah bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi dan dekripsi. Teknik ini untuk mengkonversi data ke bentuk kode-kode tertentu agar informasi tidak dapat terbaca oleh siapapun kecuali pihak yang berhak. Salah satu metode kriptografi yang biasa digunakan adalah algoritma simetris yang menggunakan kunci yang sama saat melakukan enkripsi dan dekripsi, sehingga informasi sulit dipahami maknanya [7].

Ilmu kriptografi dapat diklasifikasikan atas 2 bagian:

a. Kriptografi klasik
b. Kriptografi modern

B. Proses Kriptografi

Kriptografi mempunyai 2 proses yaitu enkripsi dan dekripsi. Enkripsi (fungsi E) adalah proses pengubahan *plaintext* menjadi *ciphertext*. Sedangkan dekripsi (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli. Komponen kripografi ada 2 yaitu *plaintext* (data asli) dan *ciphertext* (data yang telah diacak) [8].



Gambar 2. Diagram Proses Enkripsi dan Dekripsi

1. Bit Geser atau *Key*

Kunci rahasia yang akan digunakan untuk mengubah pesan asli menjadi pesan rahasia [9].

2. Proses Enkripsi dan Proses Dekripsi

Proses Enkripsi yaitu proses pengacakan data menggunakan sebuah *key* agar tidak dapat dibaca oleh pihak lain. Sedangkan proses dekripsi adalah proses mengembalikan data yang telah diacak menjadi data asli dengan sebuah *key*. Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang dikirimkan diubah sedemikian rupa, sehingga tidak mudah disadap. Jadi, enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (*encryption*) (Budi Raharjo, 2002). *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah. Terminologi yang lebih tepat digunakan adalah "*encipher*". Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut dekripsi (*decryption*). Terminologi yang lebih tepat untuk proses ini adalah "*decipher*". Berdasarkan cara memproses teks (*plaintext*), *cipher* dapat dikategorikan menjadi dua jenis: *block cipher* and *stream cipher*. *Block cipher* bekerja dengan memproses data secara blok, dimana beberapa karakter/data digabungkan menjadi satu blok. Setiap proses satu blok menghasilkan keluaran satu blok juga [10].

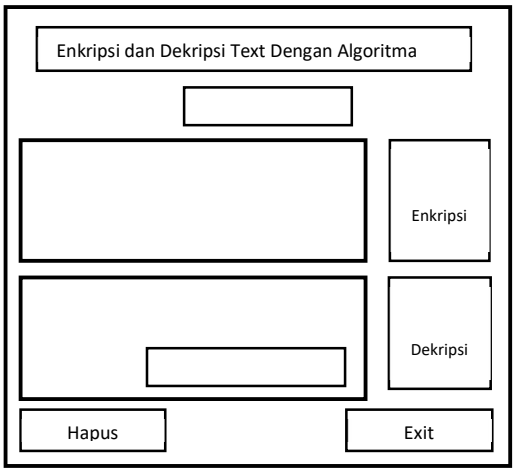
3. Perancangan Perangkat Lunak

Perancangan perangkat lunak terdiri dari desain antar muka perangkat lunak dan *source* kode program perangkat lunak. Perancangan desain antar muka bertujuan agar pengguna mudah dalam menggunakan perangkat lunak dalam melakukan enkripsi dan dekripsi pesan

baik berupa *text*. Perangkat lunak dibangun dengan bantuan aplikasi Visual Basic.

Gambar 3. Visual Basic

Gambar 4. Adalah desain rancangan aplikasi Kriptografi, aplikasi ini nantinya akan dibangun dengan Visual Basic seperti yang dapat dilihat pada Gambar 3.



Gambar 4. Desain Rancangan Aplikasi Kriptografi

Source Code

```
Private Sub Command1_Click()
If Text5.Text = "" Then

MsgBox "Anda Belum Menginputkan Bit Geser...!!", vbCritical, "Warning"
Text5.SetFocus
End If
Var = Text5.Text
Text2 = ""
If Var < 26 Then
N = Len(Trim(Text1))
For i = 1 To N
C = Mid(Text1, i, 1)
P = Chr(Asc(C) + Var)
If Asc(P) > 90 Then
Text2.SelText = Chr(64 + (Asc(P) - 90))
Else
Text2.SelText = P
Text1.Enabled = True
End If
Next
Else
MsgBox " Maksimal Bit Hanya 26...!!!", vbOKOnly + vbInformation, "Peringatan"
Text5 = ""
End If
End Sub

Private Sub Command2_Click()
Var = Text5.Text
Text4 = ""
If Var < 26 Then
N = Len(Trim(Text3))
For i = 1 To N
C = Mid(Text3, i, 1)
P = Chr(Asc(C) + 26 - Var)
If Asc(P) > 90 Then
Text4.SelText = Chr(64 + (Asc(P) - 90))
Else
Text4.SelText = P
End If
Next
Else
MsgBox " Data Anda Salah..!!!", vbOKOnly + vbInformation, "Peringatan"
Text5 = ""
End If
End Sub

Private Sub Command3_Click()
Text1 = ""
Text2 = ""
Text3 = ""
Text4 = ""
Text5 = ""
Text5.SetFocus
End Sub

Private Sub Command4_Click()
End
End Sub

Private Sub Text1_KeyPress(KeyAscii As Integer)
Text1.SetFocus
If KeyAscii = 8 Then Exit Sub
KeyAscii = Asc(UCase(Chr(KeyAscii)))
```

```
        If Not (KeyAscii >= 65 And KeyAscii
        <= 90) Then
        KeyAscii = 0
        End If
        End Sub

        Private Sub Text2_KeyPress(KeyAscii
As Integer)
        If KeyAscii = 8 Then Exit Sub
        KeyAscii                          =
Asc(UCase(Chr(KeyAscii)))
        If Not (KeyAscii >= 65 And KeyAscii
<= 90) Then
        KeyAscii = 0
        End If
        End Sub

        Private Sub Text3_KeyPress(KeyAscii
As Integer)
        Text3.SetFocus
        If KeyAscii = 8 Then Exit Sub
        KeyAscii                          =
Asc(UCase(Chr(KeyAscii)))
        If Not (KeyAscii >= 65 And KeyAscii
<= 90) Then
        KeyAscii = 0
        End If
        End Sub
```

4. Hasil

Berikut ini proses enkripsi dan dekripsi *text* dengan aplikasi Visual Basic yang telah dibuat, dan juga pada tahap ini akan dijelaskan bagaimana pengujiannya dilakukan dengan tujuan untuk mendapatkan hasil enkripsi dan dekripsi yang valid.

Gambar 5. Antar Muka Enkripsi dan Dekripsi *Text*

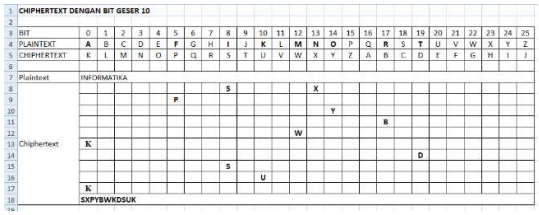
Gambar 5 menunjukkan gambar antar muka atau tampilan aplikasi enkripsi dan dekripsi *text* dengan menggunakan bit geser atau *key* tertentu. Pada Gambar 6 akan dilakukan enkripsi dengan nama INFORMATIKA dengan bit geser 10.

Gambar 6. Proses Enkripsi dan Dekripsi *Text*

Pada Gambar 6 dapat dijelaskan dengan bit geser 10 bahwa *Plaintext* (data asli) dengan nama INFORMATIKA telah berhasil dilakukan enkripsi, pada *chipertext* (data acak) dapat dilihat hasilnya menjadi tulisan acak yang tidak ada makna yaitu SXPYBWKDSUK, kemudian aplikasi pada gambar 6 juga dapat melakukan dekripsi atau membalikkan kembali data yang telah dacak.

5. Pengujian

Pengujian dilakukan untuk menguji apakah aplikasi telah valid dalam melakukan enkripsi dan dekripsi *text* dengan algoritma subtitusi *chipper*. Pengujian dilakukan dengan bantuan Microsoft Excel yiatu sebagai berikut.



Tabel 2. Pengujian Aplikasi Enkripsi dengan *Plaintext* INFORMATIKA

Setelah dilakukan pengujian, dari Tabel 2 dengan *Plaintext* INFORMATIKA menghasilkan *Chiphertext* SXPYBWKDSUK, artinya hasil pengujian telah sama dengan hasil yang dilakukan pada aplikasi pada Gambar 6, dengan demikian dapat disimpulkan bahwa Penerapan Dekripsi dan Enkripsi *Text* dengan

Algoritma Subtitusi *Chipper* telah berhasil dilakukan dengan hasil valid atau sesuai dengan yang diharapkan.

IV. KESIMPULAN

Setelah diimplementasikan proses dekripsi dan enkripsi *text* dengan algoritma Subtitusi *Chipper* dengan *Plaintext* INFORMATIKA menggunakan aplikasi yang telah dirancang dan dibuat, kemudian telah dilakukan pengujian dengan Microsoft Excel menghasilkan hasil *Chiphertext* yang sama yaitu dengan hasil SXPYBWKDSUK, dan aplikasi yang dibangun juga dapat mengembalikan data yang sudah diacak dengan data asli yaitu dengan nama informatika, maka dapat disimpulkan bahwa Penerapan Dekripsi dan Enkripsi *Text* dengan Algoritma Subtitusi *Chipper* telah berhasil dilakukan dengan hasil valid atau sesuai dengan yang diharapkan.

Saran bagi peneliti selanjutnya agar menggunakan metode yang berbeda dalam melakukan enkripsi dan dekripsi *text*, dan menambahkan enkripsi *file* agar menghasilkan hasil yang berbeda lebih akurat atau menggunakan tools aplikasi yang berbeda misalnya menggunakan bahasa pemrograman PHP, Phyton dan lainnya.

V. REFERENCES

[1] (Atmaja Basuki, Upik Paranita, Restu Hidayat, 2016), Perancangan Aplikasi Kriptografi Berlapis Menggunakan Algoritma Caesar, Transposisi, Vigenere, Dan Blok Chiper Berbasis Mobile, *ISSN : 2302-3805,* Seminar Nasional Teknologi Informasi dan Multimedia 2016 *STMIK AMIKOM Yogyakarta, 6-7 Februari 2016.*

[2] *(*Buyung Solihin Hasugian, 2017). Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah, Jurnal Warta Edisi: 53 Juli 2017 | ISSN: 1829 – 7463.

[3] (Adnan Buyung Nasution, 2019), Implementasi pengamanan data dengan menggunakan algoritma Caesar cipher dan transposisi cipher, P-ISSN 2580-7927| E-ISSN 2615-2738 (Jurnal Teknologi Informasi) Vol.3, No.1. Juni 2019.

[4] (Muhammad Zulham, Helmi Kurniawan, Iwan Fitrianto Rahmad, 2014), Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi Rc6 Berbasis Android, Seminar Nasional Informatika 2014, Teknik Informatika, STMIK Potensi Utama.

[5] (Atmaja Basuki, Upik Paranita, Restu Hidayat, 2016), Perancangan Aplikasi Kriptografi Berlapis Menggunakan Algoritma Caesar, Transposisi, Vigenere, Dan Blok Chiper Berbasis Mobile, *ISSN: 2302-3805,* Seminar Nasional Teknologi Informasi dan Multimedia 2016 *STMIK AMIKOM Yogyakarta, 6-7 Februari 2016.*

[6] (Faturungi Muharram, At. All, 2018), Analisis Algoritma Pada Proses Enkripsi Dan Dekripsi File Menggunakan Advanced Encryption Standard (AES), Prosiding Seminar Nasional Ilmu Komputer Dan Teknologi Informasi Vol. 3, No. 2, Desember 2018
E-ISSN 2540-7902 Dan P-ISSN 2541-366X.

[7] (Arif Prayitno Nurdin Nurdin, 2017), Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia Menggunakan Algoritma *Cipher Transposition,* Jurnal elektronik system informasidan computer, Vol.3 No.1 Januari-Juni 2017.

[8] Muhammad Fairuzabadi, 2010), Implementasi Kriptografi Klasik Menggunakan Borland Delphi, Jurnal Dinamika Informatika Volume 4, Nomor 2, September 2010: 65 – 78.

[9] Muhammad Khoiruddin Harahap, 2016), Analisis Perbandinga Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad, Jurnal Nasional Informatika Dan Teknologi Jaringan, E-Issn : 2540-7600.

[10] Rifkie Primartha, 2011, Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma *Data Encryption Standard* (DES). *Jurnal Sistem Informasi (JSI), VOL. 3, NO. 2, Oktober 2011, Halaman 371-387 ISSN*