Perancangan Perangkat Lunak Kriptografi Menggunakan Algoritma Vigenere Cipher dan Triple DES Cipher

Nicolaus Ribut Waidy, Wahyu Sindu Prasetya
[1,2]STMIK Pontianak; Jln. Merdeka Barat No. 372 Pontianak,
telp/fax(0561)73555/(0561)737777
[3]Jurusan TeknikInformatika, STMIK Pontianak
e-mail: **nicolausr56@gmail.com, wahyusinduprasetya@gmail.com**

Abstrak

Perkembangan teknologi informasi memiliki dampak positif dan negatif. Salah satu dampak negatifnya adalah bertambahnya banyak kasus keamanan komputer yang semakin marak terjadi. Pengguna informasi itu sendiri tidak hanya pada kalangan dewasa namun juga anak-anak dibawah umur, untuk itu diperlukan suatu aplikasi atau perangkat lunak kriptografi untuk membentengi masalah keamanan komputer tersebut. Makna kriptografi yang digunakan dalam perangkat lunak ini merupakan gabungan dari 2 algoritma yaitu algoritma Vigenere Cipher dan algoritma Triple DES Cipher yang dimana algoritma Vigenere Cipher merupaka algoritma klasik dengan cara kerja subtitusi sedangkan Triple DES Cipher merupakan algoritma modern yang merupakan pengembangan dari algoritma DES yang di enkripsi dan dekripsi sebanyak tiga kali. Perangkat lunak ini dirancang menggunakan Visual Basic 6.0 dan menghasilkan perangkat lunak yang dapat digunakan untuk menenkripsi dan mendekripsi file berupa teks dalam format txt. Perangkat lunak juga didesain dengan interface yang mudah dipahami oleh pengguna sehingga memudahkan dalam penggunaan perangkat lunak, bahkan bagi pengguna yang masih awam.
Kata kunci : *Kriptografi, Vigenere Cipher, Triple DES Cipher, Visual Basic 6.0*

Abstract

Information technology developments have positive and negative effects. One of the negative effects is the increase of cybersecurity caseswhich occurfrequently. The information users are not only adults, but also children.Therefore, an application or a cryptography software is required to defence thecybersecurity problem. The significance of cryptography whichwas used in the software was a combination of the twoalgorithms:the Vigenere Cipher and the Triple DES Cipher. The Vigenere Chipher is a classic algorithm which works substitutionally. Beside, the Triple DES Chipher is a modern algorithm; it is created from the Data Encryption Standard algorithm which has been encrypted and decrypted for three times. Thissoftware was designed by using Visual Basic 6.0in order to be able to encrypt and describe a file in txt format. In addition, this software was designed by the user-friendlyinterface which couldsimplifythe use of the software, even for lay users.
Key words: *Cryptography, Vigenere Cipher, Triple DES Cipher, Visual Basic 6.0*

1. PENDAHULUAN

Pada saat ini terjadi perkembangan yang cukup pesat di bidang teknologi, salah satunya adalah penggunaan komputerisasi dalam berbagai bidang, kemajuan teknologi informasi memberikan banyak keuntungan bagi kehidupan manusia. Tetapi keuntungan yang ditawarkan oleh teknologi informasi juga menimbulkan kejahatan seperti pencurian data dan kebocoran data. Sehingga perkembangan ilmu mengamankan data semakin ditingkatkan agar para

pengguna selalu merasa aman, telah berbagai cara dilakukan untuk mengatasi masalah keamanan data tersebut. Salah satunya melakukan penyandian terhadap data tersebut menjadi kode yang tidak mudah dimengerti. Sehingga dapat menjamin keamanan data terhadap kebocoran data yang disebabkan oleh orang-orang yang tidak berkepentingan atau pihak – pihak yang langsung berhubungan dengan basis data.

Penyandian tersebut dilakukan dengan proses enkripsi dan dekripsi terhadap informasi yang akan dikirimkan. Enkripsi dilakukan pada saat pengiriman dengan cara mengkonversi informasi asli menjadi informasi terenkripsi sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengkonversi informasi terenkripsi menjadi informasi asli. Jadi informasi yang dikirimkan selama proses pengiriman adalah data informasi terenkripsi, sehingga informasi asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Informasi asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia.

Untuk mengenkripsi dan mendekripsi data, kriptografi menggunakan suatu algoritma (*cipher*) dan kunci (*key*). *Cipher* adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi data. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data. Dalam penelitian ini penulis menggunakan algoritma kriptografi klasik *Vigenere Cipher* dan algoritma kriptografi moderen *Triple DES*. *Vigenere Cipher* adalah metode penyandian teks alfabet dengan menggunakan deretan sandi *Caesar* berdasarkan huruf-huruf pada kata kunci. *Vigenere Cipher* merupakan bentuk sederhana dari sandi substitusi *polialfabetik*. Kelebihan *Vigenere Cipher* dibandingkan dengan *Caesar Cipher* dan sandi *monoalfabetik* lainnya adalah sandi ini tidak rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi. Sedangkan *Triple DES* adalah hasil pengembangan dari *DES (Data Encryption Standard)* yaitu dengan melakukan tiga kali langkah *DES*. Kelebihan dari *Triple DES* yaitu mempunyai panjang kunci 168-bit sehingga mampu mencegah serangan *brute force.*

Pada penelitian yang dilakukan Juliadi, Bayu Prihandono, Nilamasari Kusumastuti (2013: 87-92) dalam Kriptografi Klasik Dengan Metode Modifikasi *Affine cipher* Yang Diperkuat Dengan *Vigenere cipher*. Penelitian ini mempelajari langkah pada modifikasi *Affine cipher* yang diperkuat dengan *Vigenere cipher* untuk meningkatkan keamanan pesan atau informasi dan mengetahui syarat yang harus dimiliki oleh penerima pesan yang akan melakukan dekripsi. Pada umumnya *Affine cipher* dan *Vigenere cipher* menggunakan aturan konversi berupa alfabet arab yang berjumlah 26, sedangkan pada modifikasi *Affine cipher* yang diperkuat dengan *Vigenere cipher*, penulis menambahkan beberapa karakter-karakter yaitu karakter angka dari 0 sampai 9 dan empat buah karakter lain (_ . , ‘), sehingga ukuran konversi (*m*) menjadi 40. Dari hasil penelitian didapatkan bahwa modifikasi *Affine cipher* yang diperkuat dengan *Vigenere cipher* memberikan penyandian baru dengan cara menggabungkan dua metode yaitu *Affine cioher* dengan *Vigenere cipher*, sehingga pesan atau informasi lebih sulit untuk dipecahkan oleh kriptanalisasi dibandingkan dengan penyandian yang menggunakan satu metode, misalkan hanya menggunakan *Affine cipher* atau *Vigenere cipher* saja[1].

Permanan Ginting Munthe, Adhytio Sasmita Chan (2014: 30-36), melakukan penelitian mengenai Perancangan Aplikasi Pengamanan File Dengan Memanfaatkan USB Flashdisk Sebagai Kunci Menggunakan Algoritma *Triple DES*. Dengan menggunakan metode *Tripple DES*, kata kunci akan dienkripsi terlebih dahulu pada saat disimpan untuk kemudian didekripsi pada saat proses verifikasi. Kata kunci yang dipergunakan merupakan *key* dari *flashdisk* sehingga proses keamanan datanya akan menjadi lebih baik, untuk proses enkripsi dekripsi *file flashdisk* harus dikenali terlebih dahulu jika tidak ada *flashdisk* maka proses enkripsi dan dekripsi tidak dapat dilakukan. Hasil dari penelitian ini adalah penggunaan *USB flashdisk* sebagai alat proteksi sebuah *file* dengan cara mengengkripsinya. *Flashdisk* digunakan sebagai kunci terhadap *file* yang akan diengkripsi, penggunaan *flashdisk* akan lebih aman dikarenakan

setiap *flashdisk* memiliki serial yang berbeda-beda, tanpa *flashdisk* maka *file* tidak akan bisa dienkripsi ataupun didekripsi[2].

Berdasarkan penelitian diatas sebagai suatu perbandingan dan meninjau kekurangan dan kelemahannya, maka penulis berharap dapat merancang perangkat lunak menggunakan algoritma kriptografi klasik *Vigener ecipher* dan algoritma kriptografi moderen *Triple DES cipher* sehingga dapat dimanfaatkan sebagai alat bantu dalam menjaga kerahasiaan sebuah data berlapis.

1.1 Kriptografi Vigenere Cipher

Penyandian dengan sandi Vigenere dapat dituliskan secara matematis, dengan menggunakan penjumlahan dan operasi modulus, yaitu[3]:

$C_i = (P_i + K_i) \bmod 256$

atau C = P + K kalau jumlah dibawah 256 dan - 256 kalau hasil jumlah di atas 256 dan dekripsi,

$P_i = (C_i - K_i) \bmod 256$

atau P = C - K kalau hasilnya positif dan + 26 kalau hasil pengurangan minus

Keterangan: C_i adalah huruf ke-i pada teks tersandi, P_i adalah huruf ke-i pada teks terang, K_i adalah huruf ke-i pada kata kunci, dan mod adalah operasi modulus (sisa pembagian).

Rumus enkripsi vigenere cipher :

$P_i = (C_i - K_i) \bmod 256$

atau

$C_i = (P_i + K_i) – 256$ kalau hasil penjumlahan P_i dan K_i lebih dari 256

Rumus dekripsi vigenere cipher :

$P_i = (C_i - K_i) \bmod 256$

atau

$P_i = (C_i – K_i) + 256$ kalau hasil pengurangan C_i dengan K_i minus

Dimana:

C_i = nilai desimal karakter ciphertext ke-i

P_i = nilai desimal karakter plaintext ke-i

K_i = nilai desimal karakter kunci ke-i

1.2 Kriptografi Triple DES Cipher

Triple Data Encryption Standard merupakan salah satu algoritma simetris pada kriptografi yang digunakan untuk mengamankan data dengan cara menyandikan data. Proses yang dilakukan dalam penyandian datanya, yaitu proses enkripsi dan proses dekripsi. Algoritma 3DES adalah suatu algoritma pengembangan dari algoritma DES (*Data Encryption Standard*)[4].

1.2.1 Proses Kunci

Kunci eksternal yang diinputkan akan diproses untuk mendapatkan 16 kunci internal. Pertama, Kunci eksternal yang panjangnya 64-bit disubstitusikan pada matrik kompresi PC-1. Dalam permutasi ini, setiap bit kedelapan (*parity bit*) dari delapan byte diabaikan. Hasil permutasi panjangnya menjadi 56-bit, yang kemudian dibagi menjadi dua bagian, yaitu kiri (*C0*) dan kanan (*D0*) masing-masing panjangnya 28-bit. Kemudian, bagian kiri dan kanan melakukan pergeseran bit pada setiap putaran sebanyak satu atau dua bit tergantung pada tiap putaran. Pada proses enkripsi, bit bergeser ke sebelah kiri (*left shift*). Sedangkan untuk proses dekripsi, bit bergeser ke sebelah kanan (*right shift*). Setelah mengalami pegeseran bit, *Ci* dan *Di* digabungkan dan disubstitusikan pada matriks permutasi kompresi dengan menggunakan

matriks PC-2, sehingga panjangnya menjadi 48-bit. Proses tersebut dilakukan sebanyak 16 kali secara berulang-ulang[4].

1.2.2 Proses Enkripsi

Plaintext yang diinputkan pertama akan disubatitusikan pada matriks permutasi awal (*initial permutation*) atau IP panjangnya 64-bit. Kemudian dibagi menjadi dua bagian, yaitu kiri(*L*) dan kanan (*R*) masing-masing panjangnya menjadi 32-bit. Kedua bagian ini masuk ke dalam16 putaran DES. Satu putaran DES merupakan model jaringan Feistel, secara matematis jaringan Feistel dinyatakan sebagai berikut[4]:

$$L_i = R_{i-1} \qquad ; 1 \le i \le 16$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

1.2.3 Proses Dekripsi

Proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah *k1, k2, ..., k16* maka pada proses dekripsi urutan kunci internal yang digunakan adalah *k16, k15, ..., k1*[4].

1.2.4 Proses Enkripsi dan Dekripsi

Proses enkripsi dan dekripsi algoritma 3DES dapat dicapai dengan beberapa cara, yaitu[4]:

Tabel 1.1 Proses Enkripsi dan Dekripsi Triple DES

Cara	Enkripsi	Deskripsi
1	DES – EDE2 • K1 ≠ K2, K3 = K1 • C = E [D {E (P, K1), K2}, K3]	DES – DED2 • K1 ≠ K2, K3 = K1 • P = D [E {D (C, K3), K2}, K1]
2	DES – EEE2 • K1 ≠ K2, K3 = K1 • C = E [E {E (P, K1), K2}, K3]	DES – DDD2 • K1 ≠ K2, K3 = K1 • P = D [D {D (C, K3), K2}, K1]
3	DES – EDE3 • K1 ≠ K2 ≠ K3 ≠ K1 • C = E [D {E (P, K1), K2}, K3]	DES – DED3 • K1 ≠ K2 ≠ K3 ≠ K1 • P = D [E {D (C, K3), K2}, K1]
4	DES – EEE3 • K1 ≠ K2 ≠ K3 ≠ K1 • C = E [E {E (P, K1), K2}, K3]	DES – DDD3 • K1 ≠ K2 ≠ K3 ≠ K1 • P = D [D {D (C, K3), K2}, K1]

2. METODE PENELITIAN

Bentuk penelitian yang penulis gunakan dalam penelitian ini adalah studi literature dan eksperimen murni. Penulis melakukan kajian yang berkaitan erat dengan permasalahan yang hendak dipecahkan serta mendefinisikan masalah dengan melakukan eksperimen. Selain itu penulis juga mencari referensi dan informasi yang diperlukan dari buku-buku dan artikel-artikel di Internet. Referensi dan informasi tersebut merupakan dasar pembuatan aplikasi oleh

penulis. Metode penelitian yang digunakan oleh penulis adalah metode eksperimen, yaitu melakukan percobaan (ujicoba) serta manipulasi objek secara langsung, untuk mendapatkan hasil yang memuaskan.

Jenis data terdiri dari dua jenis, yaitu data primer dan data sekunder. Data primer adalah data yang berasal dari sumber asli atau pertama. Data ini harus melalui sumber data, yaitu orang yang dijadikan sebagai sumber informasi atau data. Sedangkan data sekunder adalah data yang sudah tersedia sehingga dapat dicari dan dikumpulkan secara langsung. Data ini dapat dari internet, perpustakaan dan sumber lainnya.

Metode pengumpulan data yang digunakan peneliti adalah studi dokumentasi, yaitu peneliti mengumpulkan serta mempelajari bahan-bahan tertulis yang berhubungan dengan penggunaan gabungan algoritma Vigenere Cipher, dan Triple DES Cipher yang didapat melalui artikel, buku, *e-book* dan pencarian di internet terhadap materi metode Kriptografi algoritma Vigenere Cipher, dan Triple DES Cipher**.**

2.1 Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan oleh penulis adalah :

a. Dokumentasi

   Dokumentasi dilakukan untuk mencari data berupa gambar, tulisan dan dokumentasi lainnya mengenai hal-hal atau variabel yang diperlukan. Penulis mempelajari buku-buku, majalah, skripsi, jurnal, pencarian di Internet serta referensi yang ada yang berhubungan dengan teori-teori kriptografi, algoritma Vigenere cipher, dan Triple DES cipher serta perancangan perangkat lunak.

b. Observasi (*observation*), dilakukan dengan cara menguji hasil dari permasalahan dengan mencari banyak referensi contohnya dengan melakukan pengamatan dan menganalisis *website* yang telah ada sebagai referensi yang tepat untuk penulisan.

2.2 Instrumen dan Variabel Penelitian

Adapun intrumen atau alat (tools) yang digunakan penulis dalam penelitian yaitu menggunakan algoritma dan *flowchart* (bagan alir). Dalam penelitian ini yang menjadi variable penelitian adalah Perancangan Perangkat Lunak Kriptografi Menggunakan Vigenere Cipher, dan Triple DES Cipher.

2.3 Metode Perancangan Perangkat Lunak

Penulis menggunakan metode perancangan RAD (*Rapid Application Development*) karena proses perkembangan perangkat lunak ini menekankan pada siklus perkembangan yang singkat. RAD adalah sebuah strategi pengembangan sistem yang menekankan kecepatan dalam pengembangan melalui keterlibatan pengguna dalam pembangunan secara cepat, interaktif, dan *incremental* dari serangkaian *prototype* dari suatu sistem yang dapat berkembang menjadi suatu sistem akhir atau versi tertentu[5].

2.4 Metode Pengujian Perangkat Lunak

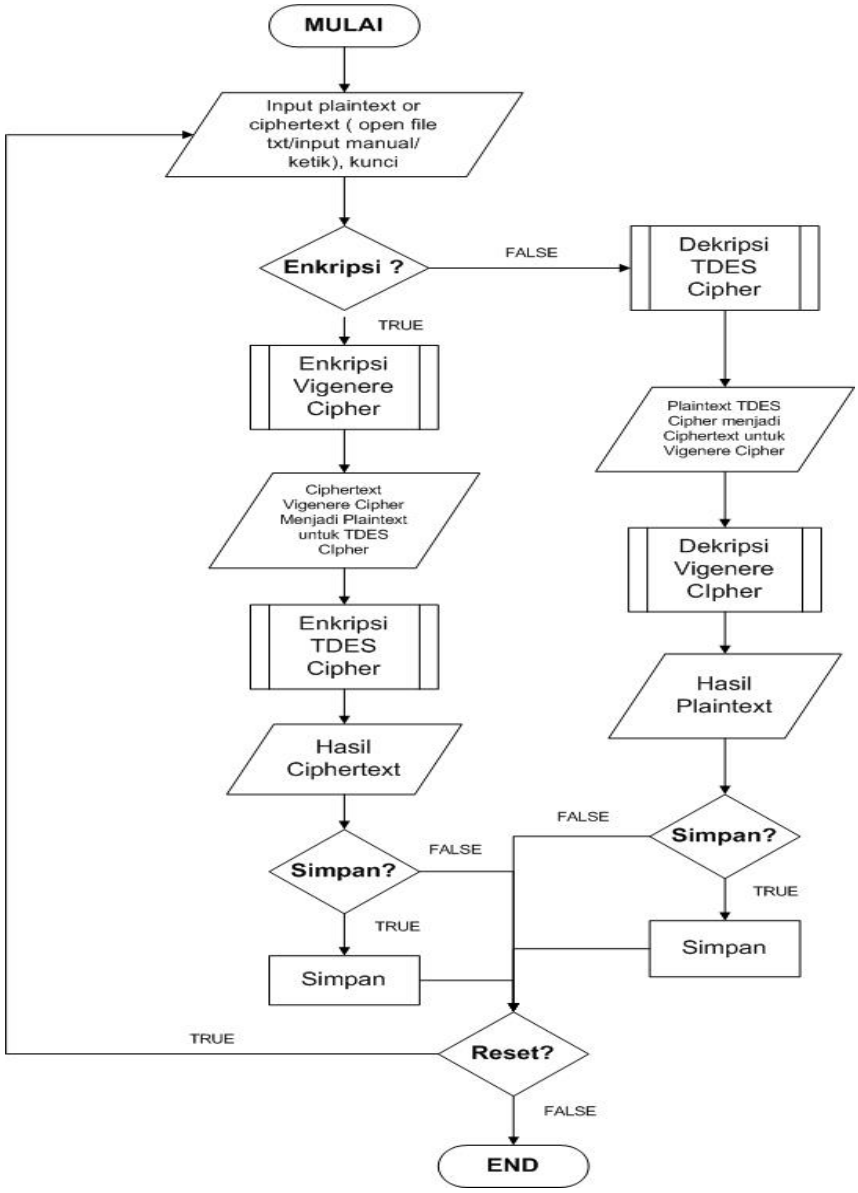
Untuk melakukan pengujian perangkat lunak kriptografi yang menggunakan algoritma gabungan *Vigenere Cipher* dan *Triple DES Cipher*, penulis menggunakan metode *black-box* dan proses formal *vertification*. Pengujian dilakukan terhadap fungsi-fungsi yang ada dengan menginput data masukan dan meneliti data hasil outputnya.

3. HASIL DAN PEMBAHASAN

Pada perancangan perangkat lunak kriptografi dalam penelitian ini penulis menggunakan algoritma Vigenere Cipher dan Triple DES Cipher dengan cara ke empat yang menerapkan 3 (tiga) kali proses enkripsi pada enkripsi file, 3 (tiga) kali proses dekripsi pada dekripsi file dan 3 (tiga) kunci yang berbeda.

Perangkat kriptografi yang dirancang menggunakan 2 kriptografi yaitu Vigenere Cipher dan Triple DES Cipher. Pesan yang dikirimkan terlebih dahulu di Enkripsi menggunakan Vigenere Cipher kemudian hasil dari Enkripsi tersebut di Enkripsi kembali menggunakan Triple DES Cipher. Begitu juga sebaliknya untuk proses dekripsi bahwa pesan yang diterima terlebih dahulu didekripsi menggunakan Triple DES Cipher dan kemudian didekripsi lagi menggunakan Vigenere Chipper.

Berikut ini gambar flowchart proses enkripsi dan dekripsi kriptografi gabungan algoritma Vigenere Cipher dan algoritma Triple DES Cipher adalah sebagai berikut :



Gambar 3.1 Flowchart Algoritma Kriptografi Gabungan

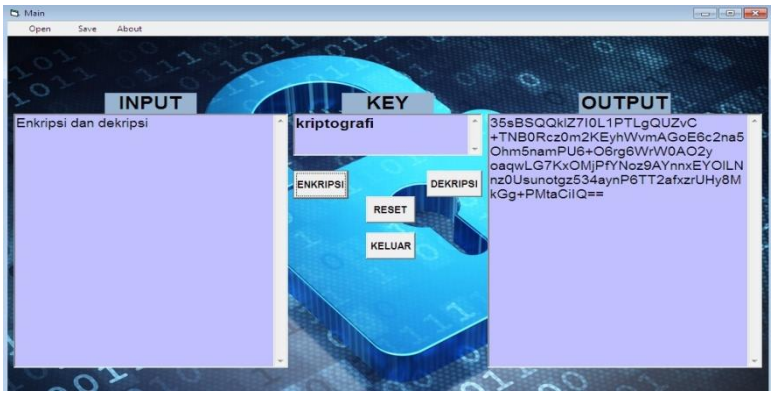
Vigenere Cipher dan Triple DES Cipher

Algoritma untuk kriptografi gabung Vigenere Cipher dan Triple DES Cipher adalah sebagai berikut :

a. Mulai.
b. Input plaintext dapat melalui menu open file (format file .txt) atau diketik secara manual, kemudian diinputkan juga kunci untuk enkripsi atau dekripsi.
c. Setelah file diinputkan, user diberikan pilihan apakah akan menenkripsi atau mendekripsi file. Jika user menenkripsi file maka langkah-langkah enkripsi dimulai dari enkripsi menggunakan Vigenere Cipher kemudian dilanjutkan enkripsi menggunakan Triple DES Cipher, dan sebaliknya jika user mendekripsi file maka langkah-langkah dekripsi dimulai dari dekripsi menggunakan Triple DES Cipher kemudian dilanjutkan dekripsi menggunakan Vigenere Cipher.
d. Hasil dari enkripsi berupa ciphertext dan hasil dari dekripsi berupa plaintext.
e. User bisa memilih apakah ingin menyimpan hasil enkripsi/dekripsi atau tidak.
f. Selanjutnya user bisa memulai langkah dari awal dengan menggunakan tombol reset, jika tidak maka user bisa menutup aplikasi.
g. Selesai

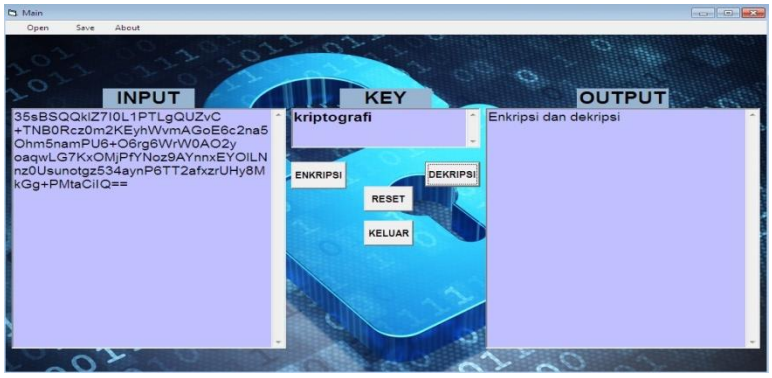
Berikut adalah contoh dari penggunaan perangkat lunak untuk menenkripsi dan mendekripsi file text:

a. Pengujian untuk kurang dari lima kata



Gambar 3.2 Pengujian Enkripsi Pertama

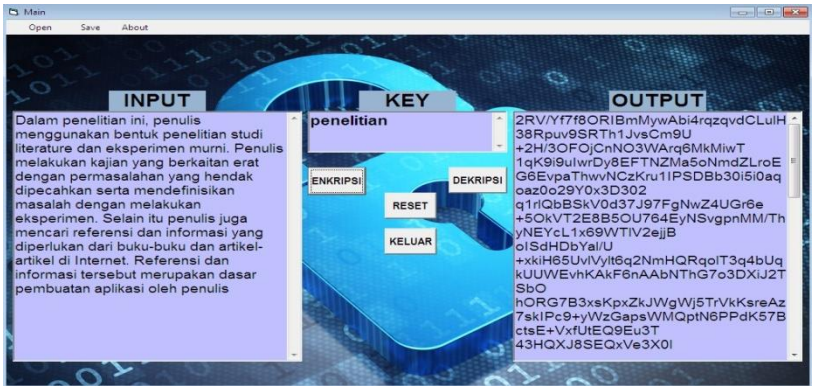
Waktu yang dibutuhkan untuk melakukan enkripsi pada plaintext diatas tidak memerlukan waktu yang lama untuk melakukan enkripsi karena panjang dari plaintext tersebut masihlah belum panjang dan hanya memiliki karakter kurang dari 5 kata.



Gambar 3.3 Pengujian Dekripsi Pertama

Waktu yang dibutuhkan untuk melakukan dekripsi pada ciphertext diatas tidak memerlukan waktu yang lama untuk melakukan dekripsi karena panjang dari ciphertext tersebut masihlah belum panjang.

b. Pengujian untuk lebih dari 5 kata :



Gambar 3.4 Pengujian Enkripsi Kedua

Waktu yang dibutuhkan untuk melakukan enkripsi pada plaintext diatas tidak memerlukan waktu yang lama untuk melakukan enkripsi karena panjang dari plaintext tersebut masihlah belum panjang dan hanya memiliki karakter hanya 79 kata.

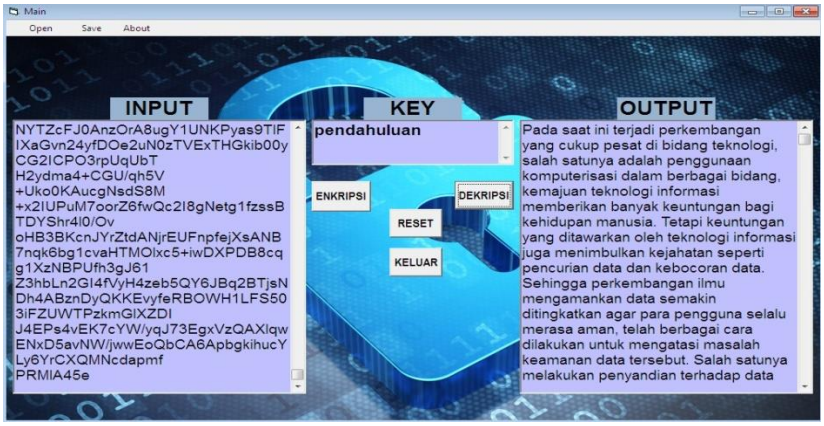
Gambar 3.5 Pengujian Dekripsi Kedua

Waktu yang dibutuhkan untuk melakukan dekripsi pada ciphertext diatas tidak memerlukan waktu yang lama untuk melakukan dekripsi karena panjang dari ciphertext tersebut masihlah belum panjang.

c. Pengujian untuk lebih dari 1000 kata :

Gambar 3.6 Pengujian Enkripsi Ketiga

Plaintext tersebut panjang katanya sebanyak 1457 kata. Waktu yang dibutuhkan untuk melakukan enkripsi pada gambar diatas sudah memiliki jeda 2 detik, semakin panjang plaintext maka akan semakin lama juga dalam melakukan enkripsi maupun dekripsi.



Gambar 4.3.7 Pengujian Dekripsi Ketiga

Ciphertext tersebut memiliki panjang karakter lebih panjang dari plaintext. Waktu yang dibutuhkan untuk melakukan dekripsi pada gambar diatas sudah memiliki jeda 3 detik untuk melakukan dekripsi jika semakin panjang ciphertext akan semakin lama juga dalam melakukan enkripsi maupun dekripsi.

Pengujian enkripsi dan dekripsi file memerlukan waktu dalam melakukan penyandian file sehingga file yang memiliki ukuran data besar akan memerlukan waktu yang lebih lama dari ukuran file yang kecil.

Berikut adalah tabel hasil pengujian perangkat lunak kriptografi menggunakan algoritma vigenere Cipher dan Triple DES Cipher :

a. Pengujian pada Halaman Utama

Pengujian pada Halaman Utama bertujuan untuk mengetahui apakah fungsi yang digunakan untuk proses pengujian pada aplikasi kriptografi berfungsi baik atau tidak.

Nama Projek		Pengujian Pada Halaman Utama		
Mulai Percobaan		23 Febuari 2017		
Percobaan berakhir		23 Febuari 2017		
Nama Penguji		Nicolaus Ribut Waidy		
Desripsi		Menguji Halaman Utama		
Pre-kondisi		Pilih		
ID	Langkah Percobaan	Test Data	Hasil	Kesimpulan
1	Masuk ke dalam Form Utama	Jalankan aplikasi	Menu Utama Tampil	Pass
2	Masuk ke dalam Form About	Klik Menu About	Menu About Tampil	Pass

b. Pengujian Enkripsi

Pengujian Enkripsi bertujuan untuk mengetahui apakah fungsi yang digunakan untuk proses pengujian pada aplikasi kriptografi berfungsi baik atau tidak.

Nama Projek		Pengujian Enkripsi		
Mulai Percobaan		23 Febuari 2017		
Percobaan berakhir		23 Febuari 2017		
Nama Penguji		Nicolaus Ribut Waidy		
Desripsi		Menguji Enkripsi		
Pre-kondisi		Melakukan Input plaintext dan kunci		
ID	Langkah Percobaan	Test Data	Hasil	Kesimpulan
1	Melakukan Enkripsi	Masukan plaintext dan kunci lalu klik tombol enkripsi	Berhasil melakukan enkripsi	Pass
2	Membersihkan isi dari textbox	Klik tombol Reset	Textbox input dan output kosong	Pass
4	Menutup Aplikasi	Klik tombol Keluar	Aplikasi ditutup	Pass

c. Pengujian Dekripsi

PengujianDekripsi bertujuan untuk mengetahui apakah fungsi yang digunakan untuk proses pengujian pada aplikasi kriptografi berfungsi baik atau tidak.

Nama Projek		Pengujian Dekripsi		
Mulai Percobaan		23 Febuari 2017		
Percobaan berakhir		23 Febuari 2017		
Nama Penguji		Nicolaus Ribut Waidy		
Desripsi		Menguji Dekripsi		
Pre-kondisi		Melakukan Input ciphertext dan kunci		
ID	Langkah Percobaan	Test Data	Hasil	Kesimpulan
1	Melakukan Dekripsi	Mengisi Data/Ciphertext yang	Berhasil melakukan	Pass

		ingin enkripsi. lalu, tekan dekripsi	dekripsi	

d. Pengujian Pada Jumlah Kata yang Dienkripsi

Pengujian pada jumlah kata yang dienkripsi bertujuan untuk mengetahui apakah fungsi yang digunakan untuk proses pengujian pada aplikasi kriptografi berfungsi baik atau tidak.

Nama Projek	Pengujian Pada Jumlah Kata yang Dienkripsi			
Mulai Percobaan	23 Febuari 2017			
Percobaan berakhir	23 Febuari 2017			
Nama Penguji	Nicolaus Ribut waidy			
Deskripsi	Menguji Enkripsi			
Pre-kondisi	Melakukan Input plaintext dan kunci			
ID	Langkah Percobaan	Test Data	Hasil	Kesimpulan
1	Menginput pesan/plaintext dan kunci untuk melakukan enkripsi, klik tombol enkripsi	Jumlah kata dienkripsi kurang dari 5 kata	Dapat dienkripsi dengan cepat	Pass
2	Menginput pesan/plaintext dan kunci untuk melakukan enkripsi, klik tombol enkripsi	Jumlah kata dienkripsi lebih dari 50 kata	Dapat dienkripsi dengan cepat	Pass
3	Menginput pesan/plaintext dan kunci untuk melakukan enkripsi, klik tombol enkripsi	Jumlah kata dienkripsi sebanyak 1457 kata	Memerlukan waktu sebanyak 2 detik	Pass

e. Pengujian Pada Jumlah Huruf yang Didekripsi

Pengujian pada jumlah huruf yang didekripsi bertujuan untuk mengetahui apakah fungsi yang digunakan untuk proses pengujian pada aplikasi kriptografi berfungsi baik atau tidak.

Nama Projek	Pengujian Pada Jumlah Huruf yang Didekripsi			
Mulai Percobaan	23 Febuari 2017			
Percobaan berakhir	23 Febuari 2017			
Nama Penguji	Nicolaus Ribut Waidy			
Deskripsi	Menguji Dekripsi			
Pre-kondisi	Melakukan Input ciphertext dan kunci			
ID	Langkah Percobaan	Test Data	Hasil	Kesimpulan
1	Menginput ciphertext dan kunci untuk melakukan dekripsi, klik tombol enkripsi	Jumlah kata dienkripsi sebanyak 152 karakter	Dapat dienkripsi dengan cepat	Pass
2	Menginput ciphertext dan kunci untuk melakukan enkripsi, klik tombol enkripsi	Jumlah kata dienkripsi sebanyak 1208 karakter	Dapat dienkripsi dengan cepat	Pass

3	Menginput ciphertext dan kunci untuk melakukan enkripsi, klik tombol enkripsi	Jumlah kata dienkripsi sebanyak 28736 karakter	Memerlukan waktu sebanyak 3 detik	Pass

f. Pengujian Menu Aplikasi

Pengujian menu aplikasi bertujuan untuk mengetahui apakah fungsi yang digunakan untuk proses pengujian pada aplikasi kriptografi berfungsi baik atau tidak.

Nama Projek	Pengujian Menu Aplikasi			
Mulai Percobaan	23 Febuari 2017			
Percobaan berakhir	23 Febuari 2017			
Nama Penguji	Nicolaus Ribut Waidy			
Deskripsi	Menguji Menu Apliksi			
Pre-kondisi	Klik			
ID	Langkah Percobaan	Test Data	Hasil	Kesimpulan
1	Membuka file yang akan dienkripsi atau didekripsi. Format file .txt	Klik menu open pada apliksi untuk membuka file yang akan dienkripsi atau didekripsi	Bisa membuka file	Pass
2	Menyimpan file yang sudah dienkripsi atau didekripsi	Klik menu save untuk menyimpan hasil enkripsi maupun dekripsi	Bisa menyimpan file	Pass
3	Menampilkan form About	Klik menu About pada aplikasi	Form About bisa ditampilkan	Pass

4. KESIMPULAN

Dalam penelitian ini memberikan kesimpulan yang mengindikasikan diperlukannya pengamanan data dengan menggunakan teknik kriptografi. Teknik penyandian kriptografi klasik pada kenyataanya masih layak untuk digunakan sebagai sistem keamanan suatu pesan, namun haruslah diperkuat dengan metode tertentu, salah satunya adalah dengan memperkuat penyandian kriptografi klasik dengan kriptografi modern.

Sistem penyandian seperti ini menghasilkan suatu metode kriptografi enkripsi yang memiliki kelebihan sebagai berikut :

a. Merupakan suatu sistem penyandian klasik yang lebih baik, karena menggabungkan konsep subtitusi yang dimiliki oleh kriptografi klasik dan konsep kriptografi modern dengan pergeseran bit yang dimiliki oleh sandi kriptografi Triple DES Cipher.

b. Memperkecil kemungkinan pembobolan sandi klasik oleh kriptanalis dan meningkatkan kerumitan hubungan antara plainteks dan cipherteks.
c. Sistem penyandian terbilang sederhana dan mudah untuk diimplementasikan karena hanya berdasarkan metode pergeseran bit dan metode pergantian karakter alphabet atau subsitusi, namun sandi ini terbilang cukup rumit untuk dapat dipecahkan.

5. SARAN

Mekanisme enkripsi dan dekripsi yang digunakan dalam penelitian kali ini memang masih terbilang cukup sederhana, akan tetapi diharapkan dapat berguna sebagai langkah awal untuk masuk ke dalam dunia kriptografi, khususnya dalam implementasi pengamanan pesan dengan menggunakan penyandian klasik. Untuk kedepannya, diharapkan penelitian ini dapat dikembangkan, digunakan serta diterapkan pada bidang-bidang kehidupan yang lain yang lebih kompleks dan format data yang dapat disandikan juga bisa ditambah, tidak hanya data berformat text..

DAFTAR PUSTAKA

[1] Juliadi, Bayu Prihandono., dan Nilamsari Kusumastuti., 2013, Kriptografi Klasik Dengan Metode Modifikasi Affine Cipher Yang Diperkuat Dengan Vigenere Cipher, *Jurnal Bimaster*, vol.02, no.02, pp 87-92.

[2] Chan, Adhytio Sasmita., dan Munthe, Permanan Ginting., 2014, Perancangan Aplikasi Pengamanan File Dengan Memanfaatkan USB Flashdisk Sebagai Kunci Mengggunakan Algoritma Triple DES, *Jurnal Pelita Informatika Budi Darma*, vol.08, no.03, pp 30-36, ISSN : 2301-9425.

[3] Cahyadi, Tri., 2015, Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra JPEG, *Jurnal TRANSIENT*, vol.1, no.04, pp 281-288, ISSN : 2302-9927

[4] Hidayat, Akik., 2008, Enkripsi dan Dekripsi Data Dengan Algoritma 3 DES (Data Encryption Standard, *Jurnal Universitas Padjadjaran*, http://repository.unpad.ac.id/2008/1/enkripsi_dan_dekripsi_data_dengan_algoritma_3_des.pdf, diakses tanggal 25 Agustus 2016.

[5] Pressman, Roger. S., 2002, *Rekayasa Perangkat Lunak Pendekatan Praktisi (Buku Satu)*, CN Harnanigrum, ANDI, Yogyakarta.