Penerapan Kunci Berupa Gambar Pada Algoritma *Vernam Cipher* Dalam Perancangan Perangkat Lunak *Kriptografi*

Linardi[*1], Rian Oktavianus[2]
[1,2]Jurusan Teknik Informatika; STMIK Pontianak. Jl. Merdeka No.372 Pontianak, 0561-735555
E-mail: [*1]linardi99@gmail.com, [2]rian.oktavianus@stmikpontianak.ac.id

Abstrak

Keamanan data menjadi salah satu isu penting dalam perkembangan teknologi informasi saat ini. Salah satu cara yang dapat dilakuan untuk menjaga keamanan data adalah dengan menggunakan ilmu kriptografi. Proses kriptografi dilakukan dengan melakukan proses pengacakan data, sehingga file yang asli tidak mudah untuk dibaca oleh pihak yang tidak berkepentingan. Metode Vernam Cipher merupakan algoritma berjenis symmetric key kunci yang digunakan untuk melakukan enkripsi dan dekripsi yang menggunakan kunci yang sama. Dalam proses enkripsi, algoritma Vernam Cipher menggunakan cara stream cipher dimana cipher berasal dari hasil XOR antara bit plaintext dan bit key, sedangkan permutasi biner dilakukan dengan membalikan kode biner pada setiap karakter. Dalam makalah ini akan dibahas, program perangkat lunak yang dapat melakukan proses kriptografi terhadap suatu text yang diinputkan oleh user. Proses kriptografi yang terdiri dari enkripsi dan dekripsi akan menggunakan metode Vernam Cipher dan metode permutasi biner. Program dikembangkan dengan menggunakan java.

Kata Kunci – Keamanan Data, Kriptografi, Vernam Cipher

Abstract

Data security is one of the important issues in the development of information technology today. One way that can be done to maintain data security is to use cryptography. Cryptography process is done by doing the data randomization process, so that the original file is not easy to read by unauthorized parties. Vernam Cipher method is a key symmetric key algorithm that is used to perform encryption and decryption using the same key. In the encryption process, Vernam Cipher algorithm uses the stream cipher method where the cipher comes from the XOR result between the plaintext bit and the bit key, while the binary permutation is done by reversing the binary code on each character. In this paper will be discussed, software programs that can perform cryptographic processes on a text inputted by the user. Cryptographic process consisting of encryption and decryption will use Vernam Cipher method and binary permutation method. The program is developed using java.

Keywords – Data Security, Cryptography, Vernam Cipher

1. PENDAHULUAN

Seiring dengan majunya perkembangan teknologi, banyak tersedia berbagai macam teknik untuk dapat melindungi pesan atau informasi yang dirahasiakan dari orang yang tidak berhak untuk mengakses pesan tersebut seperti berhak untuk mengakses pesan tersebut seperti pencurian data dan percobaan hacking. Keamanan dan kerahasiaan adalah hal yang paling penting ketika melakukan pertukaran data tersebut baik untuk tujuan pribadi maupun kelompok. Agar data yang

dikirim tidak dapat diketahui oleh pihak yang tidak berkepentingan, maka diperlukan adanya pengamanan data mformasi yang akan diberikan. Perlindungan dengan cara kerahasiaan juga diperlukan salah satunya dilakukan dengan cara *enkripsi* data.

Dalam *kriptografi* terdapat dua konsep utama yaitu *enkripsi* dan *dekripsi*. *Enkripsi* yaitu proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awal yang dilakukan dengan menggunakan algoritma tertentu. *Dekripsi* yaitu mengubah kembali bentuk tersebut menjadi informasi awal. Penggunaan konsep *enkripsi* diperlukan untuk menjaga data yang akan dikirim melalui jaringan yang kemudian disamarkan sedemikian rupa, sehingga apabila data tersebut hilang atau dicuri oleh pihak lain, besar kemungkinan informasi awal dari data tersebut tidak dapat mereka ketahui. Data yang akan dikirim dan belum mengalami penyandian dikenal dengan istilah plaintext, dan ketika data tersebut disamarkan dengan penyandian, maka plaintext tersebut dikenal dengan istilah ciphertext.

Dalam mengamankan data terdapat banyak faktor yang mempengaruhi tingkat keamanannya, termasuk salah satunya yaitu penggunaan algoritmanya. Penelitian kali ini penulis akan dengan penerapan kunci berupa gambar pada algoritma vernam chipher untuk mengamankan data berupa text. Metode *vernam cipher* merupakan algoritma symmetric key yaitu pengunaan kunci yang sama untuk proses *enkripsi* dan proses *dekripsi*.

Dalam proses *enkripsi*, algoritma *vernam cipher* menggunakan cara steam cipher dimana cipher berasal dari hasil XOR antara bit plaintext dan bit key, sedangkan permutasi biner dilakukan dengan membalikan kode biner pada setiap karakter.

Plaintext yaitu data asli yang akan disandikan menjadi bentuk lain yang tidak diketahui oleh orang lain. Bentuk plaintext beraneka ragam berdasarkan media yang digunakan antara lain: teks, gambar, suara, video maupun IP protokol. Untuk mengubah menjadi bentuk lain plainteks memerlukan sebuah kunci. Kunci tersebut dapat berbentuk angka maupun tulisan. Media *kriptografi* yang dapat digunakan hingga saat ini dapat dibagi menjadi 5 yaitu teks, gambar, audio, video dan protokol IP[1].

Berdasarkan penelitian sebelumnya yang mengatakan sebuah kunci berbentuk angka atau tulisan maka pada makalah ini penulis akan melakukan modifikasi kunci pada kunci algoritma *vernam cipher*, dimana kunci yang akan digunakan berupa gambar atau foto yang berformat *.jpg. foto akan diproses menjadi barisan bilangan biner yang nantinya akan digunakan untuk dilakukan XOR dengan bilangan biner plaintext sehingga menjadi teks yang tak dapat dibaca atau yang biasa dikenal sebagai ciphertext. Dengan dengan penerapan kunci berupa gambar pada berupa gambar berformat *.jpg diharapkan dapat meningkatkan tingkat keamanan *kriptografi*.

JPEG (Join Photographic Expert Group) adalah sebuah format gambar yang sudah banyak digunakan untuk menyimpan file gambar dengan ukuran file yang kecil. Seperti halnya GIF, JPEG memiliki berbagai karakteristik seperti memiliki ekstensi jpg atau jpeg, mampu menayangkan kedalaman warna hingga 24-bit true color, memiliki sifat lossy saat proses kompresi sedang terjadi, dan yang terakhir biasanya digunakan untuk menyimpan gambar-gambar hasil foto. Gambar yang didapatkan dari sesi pemotretan menggunakan kamera digital merupakan sumber utama dari JPEG[2].

Sebanyak 16 juta warna tersebut berasal dari perpaduan warna merah, hijau, biru di mana masing-masing warna bernilai 0 sampai 255. Dengan demikian, kita bisa membuat 256 kombinasi merah x 256 kombinasi hijau x 256 kombinasi biru sehingga didapat 16.777.216 kombinasi warna[3].

Kombinasi warna yang sangat beragam ini lah yang mendorong penulis untuk melakukkan penelitian ini karena dianggap cukup kuat untuk mengamankan data. Hal ini

dikarenakan jika terdapat sedikit perubahan nilai warna atau posisi warna pixel yang tidak sesuai maka ciphertext tersebut akan susah dipecahkan.

2. METODE PENELITIAN

Data yang dikumpulkan dalam penelitian ini merupakan data sekunder. Data diperoleh dari telaah pustaka dan dokumen yang didapat penulis dari pustaka yang mendukung, informasi dari internet, buku-buku dan artikel dari jurnal.

1. Data Primer
   Merupakan data yang diperoleh secara langsung dari obyek penelitian atau merupakan data yang berasal dari sumber asli atau pertama. "Sumber primer adalah sumber data yang langsung memberikan data kepada pengumpul data".
2. Data sekunder
   Pengertian dari data sekunder adalah "Sumber data yang tidak langsung memberikan data kepada pengumpul data, misalnya lewat orang lain atau lewat dokumen". Data sekunder antara lain disajikan dalam bentukdata, tabel-tabel, diagram-diagram, atau mengenai topik penelitian. Data sekunder tidak didapatkan secara langsung didapatkan dari obyek penelitian, melainkan data yang berasal dari sumber yang telah dikumpulkan oleh pihak lain.

Metode penelitian dan pengembangan adalah "metode yang digunakan untuk menghasilkan produk tertentu dan menguji keefektivan produk tersebut"[4]. Metode jenis ini memerlukan waktu yang cukup lama agar menghasilkan produk yang terbaik. Namun, karena waktu yang tidak memungkinkan jika melalui semua tahapan yang ada dalam metode penelitian dan pengembangan tersebut, dalam penelitian ini penulis hanya melakukan tahap awal dari metode penelitian dan pengembangan.

Agar mempermudah dalam pengembangan sistem, maka penulis membangun sebuah sistem yang akan membantu dalam menggambarkan proses penyelesaian masalah. Metode yang sesuai dalam pengembangan sistem ini adalah metode Rapid Aplication Development (RAD). RAD adalah sebuah model proses perkembangan software sekuensial linier yang menekankan siklus perkembangan yang sangat pendek. Model ini merupakan sebuah adaptasi “kecepatan tinggi” dari model sekuensial linier di mana perkembangan cepat dicapai dengan menggunakan pendekatan kontruksi berbasis komponen.

Untuk memastikan perangkat lunak dapat berjalan sebagaimana mestinya, maka perlu dilakukan pengujian terhadap kerja perangkat lunak. Metode pengujian yang dipakai penulis adalah metode black-box. Pengujian dilakukan terhadap fungsi-fungsi yang ada dengan menginput data masukan dan meneliti data hasil outputnya. Metode Black Box adalah metode pengujian yang bertujuan untuk menunjukkan fungsi perangkat lunak tentang cara beroperasinya, agar input dan output telah berjalan sebagaimana yang diharapkan.

Pengujian perangkat lunak (*software testing*) merupakan suatu investigasi yang dilakukan untuk mendapatkan informasi mengenai kualitas dari produk atau layanan yang sedang diuji (*under test*). Pengujian perangkat lunak juga memberikan pandangan mengenai perangkat lunak secara obyektif dan independen yang bermanfaat dalam operasional bisnis untuk memahami tingkat risiko pada implementasinya. *blackbox testing* merupakan pengujian yang memungkinkan software engineer mendapatkan serangkaian kondisi input yang sepenuhnya menggunakan semua persyaratan fungsional untuk suatu program[5].

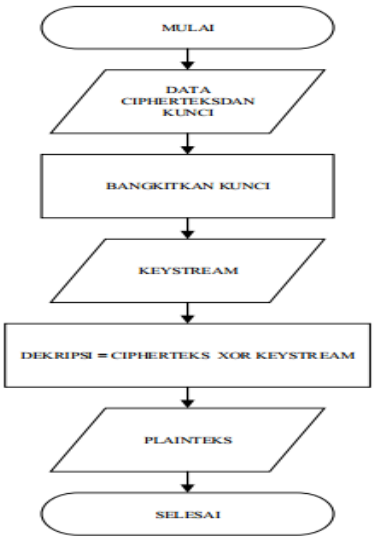
Tujuan utama pengujian adalah untuk mendeteksi kegagalan perangkat lunak sehingga cacat dapat ditemukan dan diperbaiki. Meskipun masing-masing pengujian memiliki tujuan yang berbeda perlu dilakukan pemeriksaan untuk mengetahui apakah semua elemen system telah diintegrasi dengan tepat dan melakukan fungsi-fungsi yang dialokasikan. Pengujian program dilakukan untuk melihat kesalahan (bug) yang ada dan bukan apa yang tidak terdapat pada program.

3. HASIL DAN PEMBAHASAN

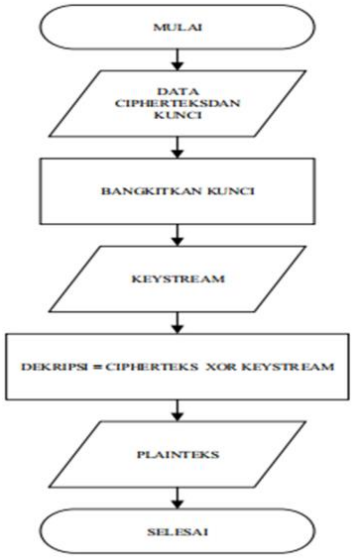
Hasil penelitian menyimpulkan agar perangkat lunak kriptgrafi dapat berjalan dengan baik sesuai rancangan yang telah dibahas sebelumnya, hasil penelitian juga mengacu semua kegiatan dalam perancangan perangkat lunak *kriptografi* dengan tool *Netbeans*. Pada hasil ini peneliti akan menerangkan pengujian keseluruhan yang telah diimplementasikan sebelumnya, hasil pengujian aplikasi meliputi : pengujian, bentuk pengujian, masukan, keluaran yang diharapkan, hasil yang didapat, dan hasil pengujian.

3.1 Analisa *Vernam Cipher*

Pada penelitan ini dibuat sebuah rancangan sistem berupa implementasi algoritma *kriptografi* vernam cipher yang dapat melakukan proses *enkripsi*/*dekripsi* data. Pada poin ini dibahas metode algoritma secara lengkap dengan prinsip kerjanya dari algoritma *vernam cipher*. Algoritma *kriptografi* vernam cipher merupakan algoritma simetri yang dalam proses enrkipsi dan *dekripsi*nya menggunakan kunci yang sama. Proses *enkripsi* dan *dekripsi* algoritma *kriptografi vernam cipher*.



Gambar 1. Diagram Alir Proses *Enkripsi* Algoritma Vernam Cipher



Gambar 2. Diagram Alir Proses *Dekripsi* Algoritma Vernam Cipher

Dari diagram alir pada Gambar 1 dan Gambar 2 dapat dilihat bahwa proses *enkripsi* maupun *dekripsi* dilakukan dengan menggunakan operasi xor, dimana pada proses *enkripsi* operasi xor dilakukan pada plainteks dan aliran bit kunci (keystream) untuk mendapatkan cipherteks. Pada proses *dekripsi* operasi xor dilakukan pada cipherteks dan aliran bit kunci (keys tream) untuk mendapatkan plainteks. Keystream merupakan aliran bit kunci yang dibangkitkan oleh pembangkit kunci (key generator). Pada Penelitian ini digunakan pembangkit kunci berupa gambar khususnya dengan format jpg.

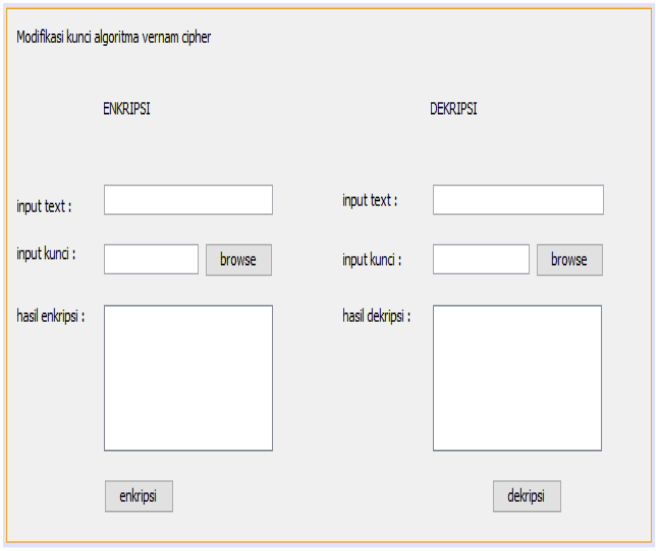
3.2 Data Modeling

Penulis menggunakan informasi yang didapat dalam tahap diatas untuk menentukan banyaknya modul dan form yang akan digunakan dalam program tersebut. Jumlah komponen yang akan terdapat dalam setiap modul dan form akan ditentukan juga. Pada bagian ini, ditampilkan terdapat beberapa pembahasan mengenai tool-tool yang digunakan untuk membuat dan menjalankan kode sumber dari perangkat lunak yang akan dibuat dan implementasi, proses yang utama dalam coding tersebut serta rancangan tampilan perangkat lunak program yang akan dibuat. Perangkat lunak ini merupakan program prototype yang dirancang hanya untuk mengamankan pesan dengan dengan penerapan kunci berupa gambar pada algoritma *vernam cipher*. Perangkat lunak ini dirancang dan digunakan untuk membantu agar pesan tidak dapat dibaca oleh orang lain yang tidak diinginkan sehingga kerahasiaan pesan tetap terjaga. Rancangan perangkat lunak ini pada intinya merupakan suatu bentuk implementasi dari system pengaman dengan dengan penerapan kunci berupa gambar pada algoritma *vernam cipher*.

Perangkat lunak *kriptografi* dengan penerapan kunci berupa gambar pada algoritma *vernam cipher* ini dirancang menggunakan bahasa pemograman java. Selain itu, penulis juga menggunakan aplikasi Microsoft visio untuk menggambar diagram proses pembentukan kunci, proses *enkripsi* dan proses *dekripsi*. Perangkat lunak modifikasi kunci algoritma *vernam cipher* ini memiliki 1 tampilan utama.

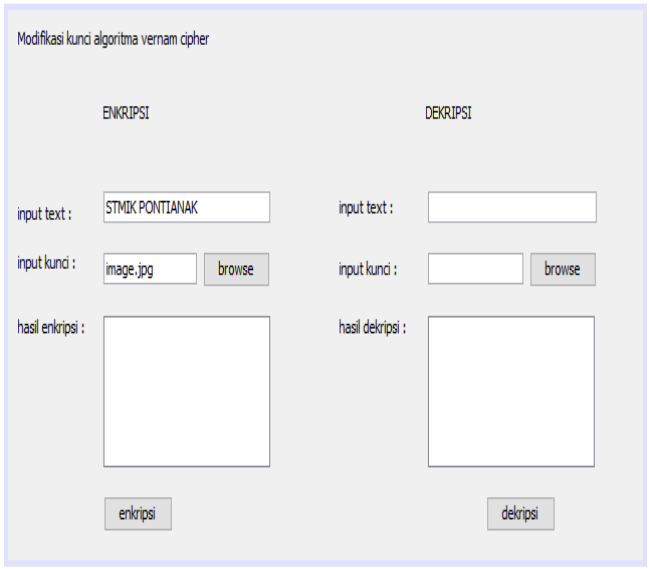
3.3 Hasil Penelitian

Pada form utama ini kita dapat melakukan *enkripsi* maupun *dekripsi*. Gambar berikut merupakan desain form utama pada saat pertama kali aplikasi dibuka.



Gambar 3. Rancangan Form Utama

Form dan modul yang sudah didefinisikan sebelumnya beserta komponen disatukan untuk membentuk suatu program utuh. Hubungan antara modul dengan form juga didefinisikan oleh penulis. Berikut ini adalah penjelesan dari gambar 3 rancangan form utama, yang diimplementasikan pada rancangan perangkat lunak modifikasi kunci algoritma *vernam cipher*.



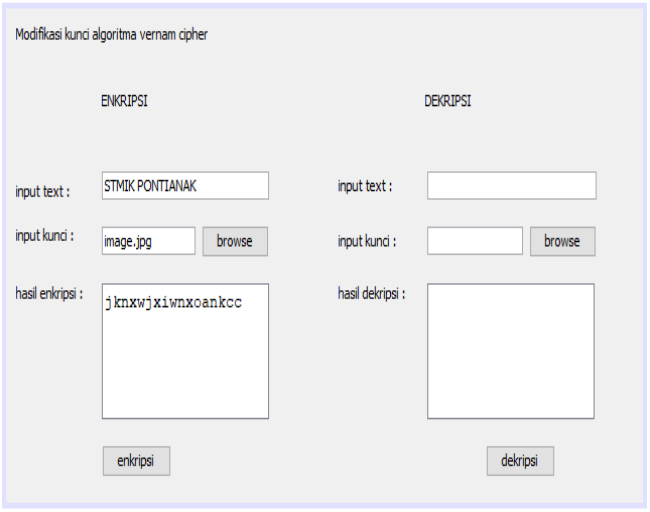
Gambar 4. proses *enkripsi*

Dari gambar diatas dapat dilihat proses input pesan plaintext pada perangkat lunak penyandian adalah sebagai berikut:

a. Input text yang akan di*enkripsi* pada textfield, teks in merupakan plaintext yang nantinya akan di*enkripsi* dan harus diisi dengan minimal 1 karakter.

b. Input karakter kunci yang digunakan untuk mengenkripsi pesan, cara menginput kunci yaitu dengan cara menekan tombol browse maka akan muncul jendela baru untuk memilih gambar yang nantinya akan dijadikan sebagai kunci.
c. Kemudian tekan atau klik tombol *enkripsi* untuk mengenkripsi pesan seperti contoh gambar dibawah ini:

Plaintext : STMIK PONTIANAK

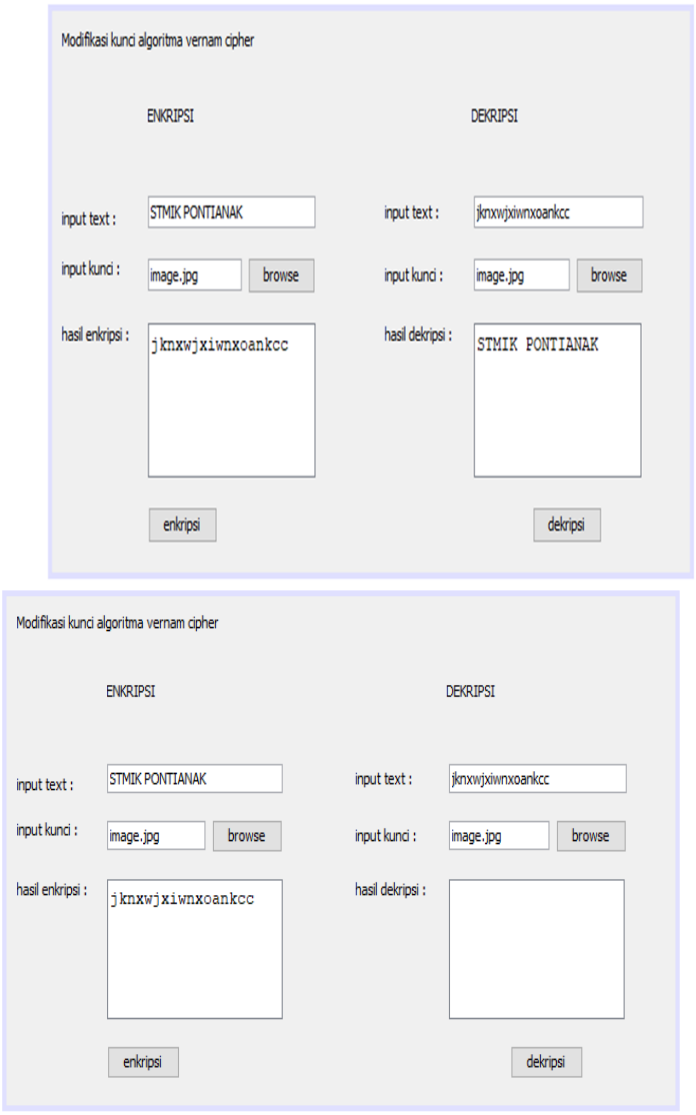


Gambar 5. hasil *enkripsi*

Dari gambar diatas merupakan hasil *enkripsi* pesan pada jendela input plaintext, setelah ditekan tombol *enkripsi* dan dilakukan proses penyandian pesan. Pada "STMIK PONTIANAK" contoh diatas didapatkan dari hasil *enkripsi*nya. Pada proses *enkripsi* pesan diatas dijalankan proses algoritma sebagai berikut:

Gambar 6. proses *enkripsi* pesan

Berdasarkan prooses diatas maka hasil dari *enkripsi* pesan yang diperoleh adalah: jknxwjxiwnxoankcc



Gambar 7. proses *dekripsi*

Dari gambar diatas dapat dilihat proses input pesan *dekripsi* pada perangkat lunak *kriptografi* sebagai berikut:

a. Input text yang akan di*dekripsi* pada textfield, text ini merupakan ciphertext yang nantinya akan di*dekripsi* dan harus diisi dengan minimal 1 karakter.
b. Input karakter kunci yang digunakan untuk mengenkripsi pesan, cara menginput kunci yaitu dengan cara menekan tombol browse maka akan muncul jendela baru untuk memilih gambar yang nantinya akan dijadikan sebagai kunci.
c. Kemudian tekan atau klik tombol *dekripsi* untuk men*dekripsi* pesan seperti contoh gambar dibawah ini:
d. Ciphertext : jknxwjxiwnxoankcc

Gambar 8. hasil *dekripsi*

Gambar diatas merupakan hasil *dekripsi* pesan pada jendela input text setelah ditekan tombol *dekripsi* dan dilakukan proses penyandian pesan. Pada contoh diatas dilakukan *dekripsi* pesan pada "jknxwjxiwnxoankcc". Pada proses *dekripsi* pesan diatas dijalankan proses algoritma sebagai berikut:

Gambar 9. proses *enkripsi* pesan

Berdasarkan proses diatas maka hasil dari *dekripsi* pesan yang merupakan plaintextnya adalah: STMIK PONTIANAK

Setelah modul dirancang ke dalam program tersebut, penulis melakukan testing pada form yang membuat modul tersebut. Setelah setiap modul dan form terbentuk dan diuji, semua modul dan form tersebut kemudian disatukan dan dilakukan pengujian kembali akan integritasnya, termasuk didalamnya pengujian valditas input tiap form. Implementasi system dalam perangkat lunak *kriptografi* ini mencakup spesifikasi kebutuhan perangkat keras (hardware) dan spesifikasi perangkat lunak (software).

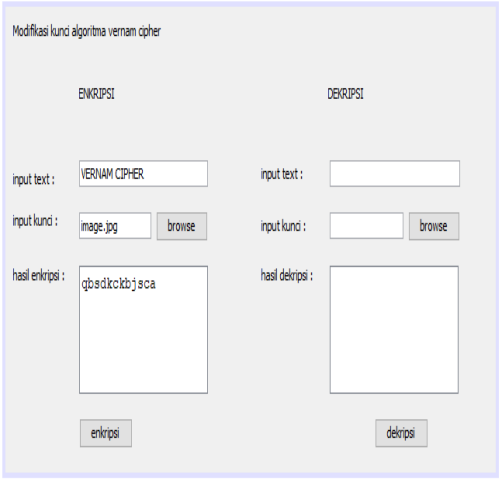
3.4 Cara Kerja Perangkat Lunak

Setelah aplikasi dijalankan akan muncul form utama yang berfungsi untuk melakukan *enkripsi* dan *dekripsi* dengan penerapan kunci berupa gambar pada algoritma vernam cipher.

Gambar 10. Tampilan Utama

Gambar 11. contoh input plaintext dan kunci

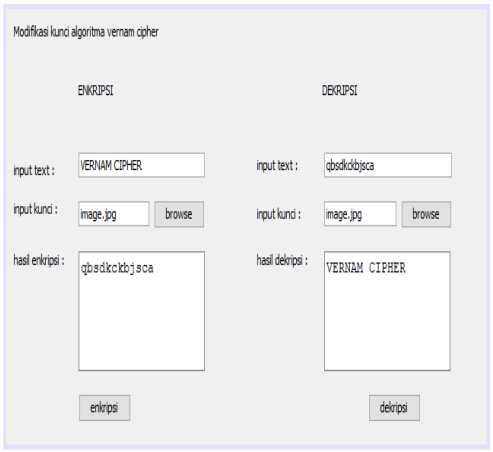
Gambar diatas dilakukan pengujian terhadap plaintext ang berisi “VERNAM CIPHER” dan menggunakan kunci berupa sebuah gambar dengan format jpg yang dapat dipilih oleh user dengan cara menekan tombol browse.



Gambar 12. tampilan hasil proses *enkripsi*

Setelah dilakukan proses *enkripsi* dengan cara menekan tombol *enkripsi*, maka didapatkan hasil ciphertext sebagai berikut : "qbsdkckbjsca"

Gambar berikut merupakan proses *dekripsi*, tampak pada hasil proses *dekripsi* didapatkan bahwa ciphertext yang di*dekripsi* akan menghasilkan plaintext kembali.



Gambar 13. tampilan hasil proses *dekripsi*

Terlihat bahwa setelah dilakukannya proses *dekripsi* dengan memasukkan ciphertext ke kolom input teks yaitu "qbsdkckbjsca" kemudian dimasukkan juga kunci berupa gambar berformat jpg yang sebelumnya digunakan untuk mengenkripsi pesan yang dapat dipilih dengan cara menekan tombol browse maka setelah ditekan tombol *dekripsi* maka akan menghasilkan kembali plaintext yaitu "VERNAM CHIPER"

4. KESIMPULAN

Dalam penelitian ini memberikan kesimpulan yang mengindikasikan diperlukannya pengamanan data dengan meggunakan teknik *kriptografi*. Teknik penyandian *kriptografi* klasik pada kenyataannya masih layak untuk digunakan sebagai sistem keamanan suatu pesan, namun haruslah diperkuat dengan metode tertentu, pada penelitian ini penulis memperkuat kemanan dengan cara menggunakan gambar sebagai kunci untuk mengenkripsi maupun mendekripsi suatu pesan.

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

a. Menggunakan gambar sebagai kunci karena selama ini kunci yang digunakan hanya sebatas text atau angka dengan demikian pesan akan tersandi lebih aman.
b. Memperkecil kemungkinan pembobolan sandi oleh kriptanalis karena kunci tidak berupa text atau angka melainkan sebuah gambar.
c. Sistem penyandian terbilang sederhana dan mudah untuk diimplementasikan karena hanya berdasarkan metode xor biner, namun sandi ini terbilang cukup sulit untuk 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 menggunakan penyandian klasik. Untuk kedepannya, diharapkan untuk format kunci yang digunakan bisa lebih berariasi tak terbatas format jpg saja serta dapat digunakan untuk mengenkripsi semua bentuk file.

UCAPAN TERIMA KASIH

Penulis ingin mengucapkan terima kasih kepada:

1. Bapak Sandy Kosasi, SE., MM., M.Kom., selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer Pontianak, selaku Dosen Pembimbing yang telah meluangkan waktu untuk membimbing dan mengarahkan sehingga penulisan jurnal dapat diselesaikan.
2. Kedua Orang Tua, Keluarga dan adik tercinta yang telah mendukung dan memberikan doa yang tulus dan dorongan semangat kepada penulis selama melakukan penulisan penelitian ini.

DAFTAR PUSTAKA

[1]. Christy Atika Sari, Eko Hari Rachmawanto, Danang Wahyu Utomo, Ramadhan Rakhmat Sani, 2016. Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan *Kriptografi Vernam Cipher* dan Bit Shiffting, Jurnal Jurusan Teknik Informatika, Universitas Dian Nuswantoro. Vol. 1 No.3.
[2]. Enterprise, J.2010. Belajar Sendiri CorelDraw X5. Elex Media Komputindo.Jakarta
[3]. Enterprise, J.2016. Pengenalan HTML dan CSS. Elex Media Komputindo.Jakarta
[4]. Sugiyono, 2008:407. Metode Penelitian Kunatitatif Kualitatif dan R&D. Bandung Alfabeta.
[5]. Pressman, Roger S., “Rekayasa Perangkat Lunak: pendekatan praktisi (Buku 1)”, Andi, Yogyakarta, 2002.