IMPLEMENTASI *ALGORITMA ONE TIME PAD* PADA PESAN

Nidia Enjelita Saragih
Dosen Universitas Potensi Utama Medan
Jln. K.L. Yos Sudarso No. 3A Medan
Sur-el: nidia.1924@gmail.com

Abstract: Easy communication process as the impact of technological developments brings new problems. That is how to ensure that communication is performed two or more parties are not accessible to persons who are not entitled to. Moreover, if the communication is done are extremely confidential. To resolve the issue of cryptographic techniques are unambiguous. Cryptography is a technique for providing the original message (plain text) into his coded message (cipher text). Cipher text is generated in the form of a code that is not understandable anymore. Cipher text which is then sent through a communication medium. The process of conversion of plain text into cipher text is called encryption, and decryption process is called instead. One of the cryptographic algorithms that have been introduced, namely algorithms One Time Pad. The encryption process uses a random key sequence is added to the plainteks that do not generate random cipherteks that are entirely random. The decryption process must use the exact same key sequence to generate a plain text.

Keywords: Cryptography, encryption, decryption, the one time pad.

Abstrak: Mudahnya proses komunikasi sebagai dampak dari perkembangan teknologi menghadirkan persoalan baru. Yaitu bagaimana menjamin agar komunikasi yang dilakukan dua atau lebih pihak tidak bisa diakses oleh orang yang tidak berhak. Apalagi jika komunikasi yang dilakukan bersifat sangat rahasia. Untuk mengatasi masalah tersebut digunakanlah teknik kriptografi. Kriptografi merupakan teknik untuk menyadikan pesan asli (plainteks) menjadi pesan tersandi (cipherteks). Cipherteks yang dihasilkan berupa kode yang tidak dapat dimengerti lagi artinya. Cipherteks inilah yang kemudian dikirimkan melalui media komunikasi. Proses pengubahan plainteks menjadi cipherteks disebut enkripsi, dan sebaliknya disebut proses dekripsi. Salah satu algoritma kriptografi yang sudah pernah diperkenalkan yaitu algoritma One Time Pad. Proses enkripsi menggunakan barisan kunci acak yang ditambahkan pada plainteks yang tidak acak menghasilkan cipherteks yang seluruhnya acak. Proses dekripsi harus menggunakan barisan kunci yang tepat sama untuk menghasilkan plainteks.

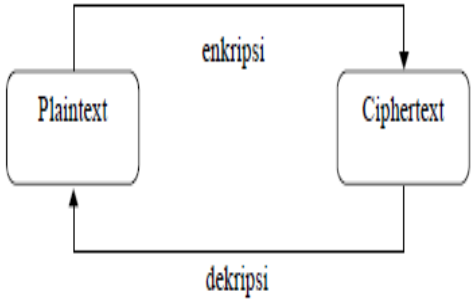
***Kata kunci** : kriptografi, enkripsi, dekripsi, one time pad.*

1. PENDAHULUAN

Perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi/data pada jarak jauh. Perkembangan dunia komputer dan pendukung perangkat lainnya yang serba digital, telah membuat data-data digital semakin banyak digunakan. Terdapat sejumlah faktor yang membuat data digital (seperti *audio, video,* citra dan teks) semakin banyak digunakan (Amin, 2014) antara lain:

1. Mudah diduplikasi dan hasilnya sama dengan aslinya.
2. Mudah untuk penduplikasian dan penyimpanan.
3. Mudah disimpan untuk kemudian diolah atau diproses lebih lanjut.
4. Serta mudah didistribusikan, baik dengan media disk maupun melalui jaringan internet

Kerahasiaan pesan atau data yang dimiliki oleh seseorang merupakan hal penting dalam pengiriman pesan agar hanya orang tertentu saja yang dapat mengakses pesan tersebut. Untuk menjaga kerahasiaan pesan diperlukan pengamanan data atau dikenal sebagai kriptografi. *Kriptografi* adalah sebuah cara untuk mengamankan informasi. Informasi yang harus dijaga kerahasiaannya haruslah diubah menjadi sebuah informasi yang tidak bisa dibaca oleh orang selain yang berhak membacanya. *Kriptografi*, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan informasi. (Nurhayati, 2013). Kriptografi disebut sebagai ilmu karena didalamnya terdapat metode (rumusan) yang digunakan, dan dikatakan sebagai seni karena karena dalam membuat suatu teknik kriptografi itu sendiri merupakan ciri tersendiri dari si pembuat dan memerlukan teknik khusus dalam mendisainnya. Orang-orang yang mendalami dan mengimplementasikan kriptografi disebut *cryptographer,* sedangkan *cryptanalysis* adalah suatu ilmu dan seni memecahkan *ciphertext* menjadi *plaintext* tanpa melalui cara yang seharusnya dan orang yang melakukannya disebut *cryptanalyst*.



Gambar 1. Proses penyandian dalam kriptografi

Kriptografi mempunyai sejarah yang panjang. Informasi yang lengkap mengenai sejarah kriptografi dapat ditemukan di dalam buku David Kahn yang berjudul *The Codebreakers*. Buku yang tebalnya 1000 halaman ini menulis secara rinci sejarah kriptografi mulai dari penggunaan kriptografi oleh Bangsa Mesir 4000 tahun yang lalu (berupa *hieroglyph* yang tidak standard pada priamid) hingga penggunaan kriptografi pada abad ke-20. Secara historis ada empat kelompok orang yang berkontribusi terhadap perkembangan kriptografi, dimana mereka menggunakan kriptografi untuk menjamin kerahasiaan dalam komunikasi pesan penting, yaitu kalangan militer (termasuk intelijen dan mata-mata), kalangan diplomatik, penulis buku harian, dan pencinta (*lovers*). Di antara keempat kelompok ini, kalangan militer yang memberikan kontribusi paling penting penting karena pengiriman pesan di dalam suasana perang membutuhkan teknik enkripsi dan dekripsi yang rumit.

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (*transposition cipher*) dan algoritma substitusi (*substitution cipher*). *Cipher* transposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan cipher substitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain. Sejarah kriptografi klasik mencatat penggunaan *cipher* transposisi oleh tentara Sparta di Yunani

pada permulaan tahun 400 SM. Mereka menggunakan alat yang namanya *scytale* (Gambar 2). *Scytale* terdiri dari sebuah kertas panjang dari daun *papyrus* yang dililitkan pada sebuah silinder dari diameter tertentu (diameter silinder menyatakan kunci penyandian). Pesan ditulis secara horizontal, baris per baris (lihat Gambar 2). Bila pita dilepaskan, maka huruf-huruf di dalamnya telah tersusun secara acak membentuk pesan rahasia. Untuk membaca pesan, penerima pesan harus melilitkan kembali melilitkan kembali kertas tersebut ke silinder yang diameternya sama dengan diameter silinder pengirim. Sedangkan algoritma substitusi paling awal dan paling sederhana adalah *Caesar cipher*, yang digunakan oleh raja Yunani kuno, Julius Caesar. Caranya adalah dengan mengganti setiap karakter di dalam alfabet dengan karakter yang terletak pada tiga posisi berikutnya di dalam susunan alfabet.

Gambar 2. Scytale

Kriptografi juga digunakan untuk tujuan keamanan. Kalangan gereja pada masa awal agama Kristen menggunakan kriptografi untuk menjaga tulisan relijius dari gangguan otoritas politik atau budaya yang dominan saat itu. Mungkin yang sangat terkenal adalah "Angka si Buruk Rupa (*Number of the Beast*) di dalam Kitab Perjanjian Baru. Angka "666" menyatakan cara kriptografik (yaitu dienkripsi) untuk menyembunyikan pesan berbahaya; para ahli percaya bahwa pesan tersebut mengacu
pada Kerajaan Romawi.

Di India, kriptografi digunakan oleh pencinta (*lovers*) untuk berkomunikasi tanpa diketahui orang. Bukti ini ditemukan di dalam buku *Kama Sutra* yang merekomendasikan wanita seharusnya mempelajari seni memahami tulisan dengan *cipher*. Pada Abad ke-17, sejarah kriptografi mencatat korban ketika ratu Skotlandia, Queen Mary, dipancung setelah surat rahasianya dari balik penjara (surat terenkripsi yang isinya rencana membunuh Ratu Elizabeth I) berhasil dipecahkan oleh seorang pemecah kode. Seperti yang telah disebutkan di atas bahwa kriptografi umum digunakan di kalangan militer. Pada Perang Dunia ke II, Pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan *Enigma*. (Gambar 3). Mesin yang menggunakan beberapa buah *rotor* (roda berputar) ini melakukan enkripsi dengan cara yang sangat rumit. Namun *Enigma cipher* berhasil dipecahkan oleh pihak Sekutu dan keberhasilan memecahkan *Enigma* sering dikatakan sebagai faktor yang memperpendek perang dunia ke-2.

Gambar 3. Mesin Enigma

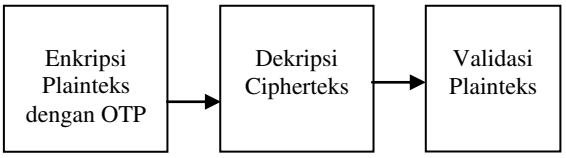
Kriptografi modern dipicu oleh perkembangan peralatan komputer digital. Dengan komputer digital, *cipher* yang lebih kompleks menjadi sangat mungkin untuk dapat dihasilkan. Tidak seperti kriptografi klasik yang mengenkripsi karakter per karakter (dengan menggunakan alfabet tradisionil), kriptografi modern beroperasi pada *string biner*.

Kriptografi modern tidak hanya berkaitan dengan teknik menjaga kerahasiaan pesan, tetapi juga melahirkan konsep seperti tanda-tangan digital dan sertifikat digital. Dengan kata lain, kriptografi modern tidak hanya memberikan aspek keamanan *confidentiality*, tetapi juga aspek keamanan lain seperti otentikasi, integritas data, dan nirpenyangkalan.

Pengembangan sejarah kriptografi terjadi pada 1976 saat Diffie dan Hellman mempublikasikan "*New Directions in Cryptography*". Tulisan ini memperkenalkan konsep revolusioner kriptografi kunci publik dan juga memberikan metode baru untuk pertukaran kunci, keamanan yang berdasar pada kekuatan masalah logaritma diskret. Meskipun Diffie dan Hellman tidak memiliki realisasi praktis pada ide enkripsi kunci publik saat itu, idenya sangat jelas dan menumbuhkan ketertarikan yang luas pada komunitas kriptografi. Pada 1978 Rivest, Shamir dan Adleman menemukan rancangan enkripsi kunci publik dan tanda tangan digital, yang sekarang disebut RSA. Rancangan RSA berdasar pada masalah faktorisasi yang sulit untuk kriptografi, dan menggiatkan kembali usaha untuk menemukan metode yang lebih efisien untuk pemfaktoran. Tahun 80-an menunjukkan peningkatan luas di area ini, sistem RSA masih aman. Sistem lain yang merupakan rancangan kunci publik ditemukan oleh Taher ElGamal pada tahun 1985. (Patil & Kumar, 2012). Salah satu algoritma lain yang pernah diperkenalkan adalah *algoritma One Time Pad*. Algoritma ini sampai saat ini dinyatakan aman karena algoritma OTP merupakan salah satu algoritma kriptografi yang tidak dapat dipecahkan. (Conelly, 2008)

2. METODOLOGI PENELITIAN

Secara umum, tahapan dari metode penelitian analisa algoritma OTP, ditunjukkan pada gambar 4.



Gambar 4. Bagan Umum Analisa *Algoritma One Time Pad*

Plainteks atau pesan asli disandikan dengan menggunakan *algoritma One Time Pad*. Sebelum proses penyandian dilakukan, terlebih dahulu dilakukan pembangkitan bilangan acak yang akan digunakan sebagai kunci. Panjang bilangan acak yang digunakan harus sama dengan panjang plainteks atau pesan asli yang disandikan.

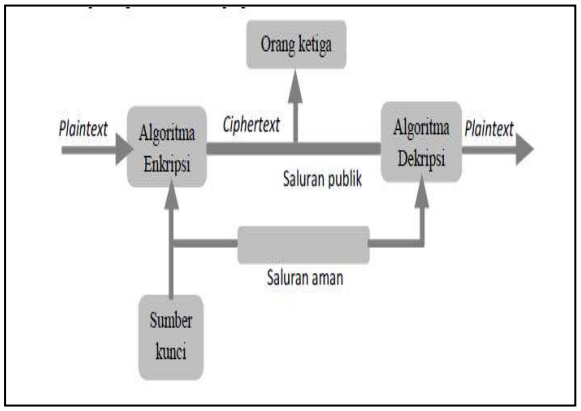
Pesan yang telah disandikan atau disebut dengan istilah Cipherteks kemudian didekripsi kembali untuk mengembalikan pesan tersandi menjadi pesan asli (plainteks). Pada implementasinya, proses ini dilakukan oleh penerima pesan agar pesan yang diterima bisa dipahami.

Proses validasi plainteks dilakukan setelah proses dekripsi dengan tujuan untuk memastikan bahwa pesan tersandi (cipherteks) bisa dikembalikan ke bentuk pesan asli (plainteks) tanpa mengalami perubahan apapun.

2.1. Algoritma One Time Pad

Kriptografi merupakan ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi. Informasi yang harus dijaga kerahasiaannya haruslah diubah menjadi bentuk yang tidak bisa dipahami oleh orang selain yang berhak menerimanya. Teknik penyandian data (kriptografi) yang diterapkan pada data maupun informasi, dilakukan dengan mengkodekan atau menyembunyikan data aslinya. (Pratiwi, dkk., 2014)

Dalam *kriptografi*, pesan atau informasi yang dapat dibaca disebut sebagai *plaintext*. Proses yang dilakukan untuk mengubah *plaintext* ke dalam *ciphertext* disebut enkripsi. *Ciphertext* adalah pesan yang tidak dapat terbaca. Proses untuk merubah *ciphertext* menjadi *plaintext* disebut proses dekripsi. Berikut merupakan gambaran dari sistem kriptografi klasik. (Muliono, 2013)



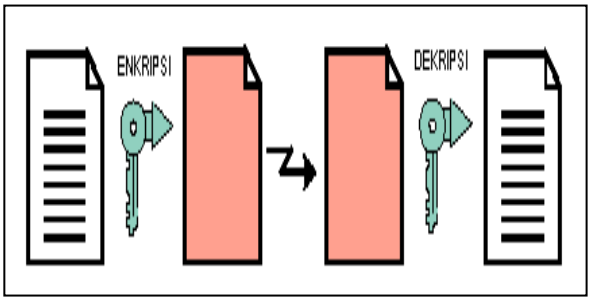
Gambar 5. Sistem Kriptografi Klasik

Dalam kriptografi dikenal dua jenis penggunaan kunci, yaitu:

1. Kunci Simetris
2. Kunci Asimetris

Kunci simetris adalah jenis kriptografi yang paling umum dipergunakan. Kunci untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan itu. Jadi pembuat pesan dan penerimanya harus memiliki kunci yang sama persis.

Siapapun yang memiliki kunci tersebut termasuk pihak-pihak yang tidak diinginkan dapat membuat dan membongkar rahasia *ciphertext*. Problem yang paling jelas disini terkadang bukanlah masalah pengiriman *ciphertext*-nya, melainkan masalah bagaimana menyampaikan kunci simetris tersebut kepada pihak yang diinginkan. Contoh algoritma kunci simetris adalah DES (*Data Encryption Standard*), RC-2, RC-4, RC-5, RC-6, TwoFish, Rijndael, *International Data Encryption Algorithm* (IDEA), *Advanced Encryption Standard* (AES), *One Time Pad* (OTP), dan lainnya .



Gambar 6. Kunci Simetris

Kelebihan kunci simetris:

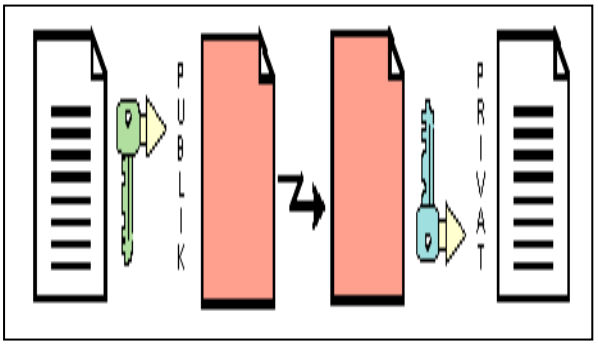
a. Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetris.
b. Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem *real-time.*

Kelemahan kunci simetris:

a. Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.
b. Permasalahan dalam pengiriman kunci itu sendiri yang disebut *"key distribution problem"* .

Kunci asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu dalam hal ini kunci privat untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya.

Dengan cara seperti ini, jika Alice mengirim pesan untuk Bob, Alice dapat merasa yakin bahwa pesan tersebut hanya dapat dibaca oleh Bob, karena hanya Bob yang bisa melakukan dekripsi dengan kunci privatnya. Tentunya Alice harus memiliki kunci publik Bob untuk melakukan enkripsi. Alice bisa mendapatkannya dari Bob, ataupun dari pihak ketiga seperti Eva.



Gambar 7. Kunci Asimetris

Teknik enkripsi asimetris ini jauh lebih lambat ketimbang enkripsi dengan kunci simetris. Oleh karena itu, biasanya bukanlah pesan itu sendiri yang disandikan dengan kunci asimetris, namun hanya kunci simetrislah yang disandikan dengan kunci asimetris. Sedangkan pesannya dikirim setelah disandikan dengan kunci simetris tadi. Contoh algoritma yang menggunakan kunci asimetris adalah RSA (merupakan singkatan penemunya yakni Rivest, Shamir dan Adleman), *Digital Signature Algorithm* (DSA), Diffie-Hellman, Kriptografi Quantum, *ElGamal*, dan lainnya.

Kelebihan kunci asimetris:

a. Masalah keamanan pada distribusi kunci dapat lebih baik .
b. Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit, maksudnya untuk berkorespondensi secara rahasia dengan banyak pihak tidak diperlukan kunci rahasia sebanyak jumlah pihak tersebut, cukup membuat dua buah kunci (disebut *public-key*) bagi para koresponden untuk mengenkripsi pesan, dan *private-key* untuk mendekripsi pesan.

Kelemahan kunci asimetris:

a. Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris .
b. Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris.

One Time Pad (OTP) adalah salah satu algoritma simetris yang ditemukan pada tahun 1917 oleh G. Vernam dan Major Joseph Mauborgne. OTP merupakan algoritma yang

relatif gampang untuk dipelajari dan sudah dinyatakan oleh para ahli kriptografi sebagai "*perfect encryption algorithm*".

Sistem *cipher One Time Pad* ini tidak dapat dipecahkan karena barisan kunci acak yang ditambahkan ke pesan *plaintext* yang tidak acak menghasilkan *ciphertext* yang seluruhnya acak. Panjang kunci harus sama dengan panjang *plaintext.* Beberapa barisan kunci yang digunakan untuk mendekripsi *ciphertext* mungkin menghasilkan pesan-pesan *plaintext* yang mempunyai makna, sehingga kriptanalis tidak punya cara untuk menentukan *plaintext* mana yang benar.

Prinsip enkripsi pada algoritma ini adalah dengan mengkombinasikan masing-masing karakter pada *plaintext* dengan satu karakter pada kunci. Oleh karena itu, panjang kunci harus sama dengan panjang *plaintext*. *Enkripsi* dapat dinyatakan sebagai penjumlahan modulo 256 (menggunakan kode ASCII 8 bit) dari satu karakter *plaintext* dengan satu karakter kunci OTP :

$$c_i = (p_i + k_i) \bmod 25 \qquad (1)$$

Dalam hal ini, p_i adalah *plaintext* ke-i, k_i adalah kunci ke-i, dan c_i adalah huruf *ciphertext* ke-i. Panjang kunci sama dengan panjang *plaintext*, sehingga tidak ada kebutuhan mengulang penggunaan kunci selama proses enkripsi. Setelah pengirim mengenkripsikan pesan dengan kunci, ia menghancurkan kunci tersebut. Penerima pesan menggunakan kunci yang sama untuk mendekripsikan karakter-karakter *ciphertext* menjadi karakter-karakter *plaintext* dengan persamaan :

$$p_i = (c_i - k_i) \bmod 256 \qquad (2)$$

2.2. Penerapan Algoritma One Time Pad

Proses enkripsi pada *algoritma One Time Pad* membutuhkan barisan bilangan acak sebagai kunci. Setiap pesan yang akan dienkripsi harus diubah ke dalam bentuk decimal untuk bisa dilakukan perhitungan, maka digunakanlah table ASCII. Sebagai contoh, untuk mengenkripsi pesan " DO " terlebih dahulu setiap karakter mengalami perubahan ke bentuk decimal menjadi " 68 79 ".

Plainteks (P) = DO

Dikonversi ke decimal menjadi :

P = 68 79

Plainteks dienkripsi dengan menggunakan bilangan acak sebagai kunci.

Kunci (k) = 23 240

Sesuai dengan persamaan enkripsi, maka plainteks diubah menjadi cipherteks:

$$c_i = (p_i + k_i) \bmod 256$$

C (1) =(68 + 23) mod 256

=91 ([ )

C (2) =(79 + 240) mod 256

=63 (**?**)

Sehingga :

P = **"DO"**

K= 23 240

C= **"[?"**

Proses dekripsi bertujuan untuk mengubah cipherteks ke bentuk semula dengan menggunakan kunci yang sama pada persamaan dekripsi berikut :

$$p_i = (c_i - k_i) \bmod 256$$

C = “ [? “

Diubah ke bentuk decimal dengan table *ASCII*

C = 91 63

K = 23 240

P(1) =(91 – 23) mod 256

=68 (D)

P(2) =(63 – 240) mod 256

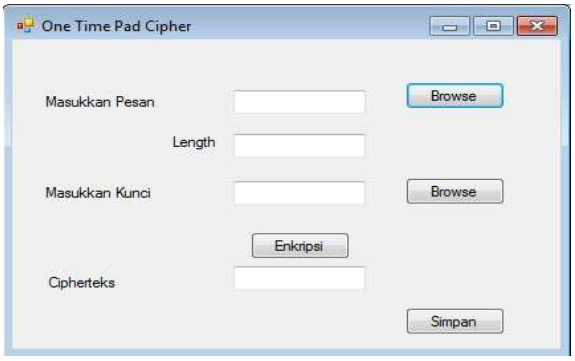
=79 (O)

P = “ DO”

Berdasarkan proses enkripsi dan dekripsi yang telah dikerjakan, diperoleh plainteks yang sama dengan plainteks yang mengalami proses enkripsi.

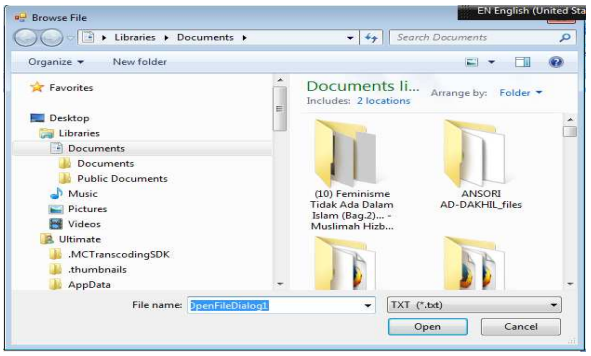
3. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini meliputi beberapa analisis dari uji coba terhadap implementasi algoritma. OTP pada pesan menggunakan pemrograman Visual Basic. Gambar 8 berikut merupakan tampilan aplikasi untuk menu enkripsi.



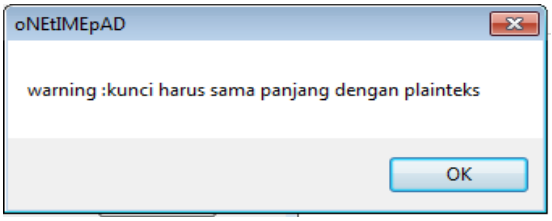
Gambar 8. Tampilan aplikasi One Time Pad Cipher

Pesan yang panjang disimpan terlebih dahulu dengan ekstensi *txt agar dapat diakses aplikasi melalui button ‘browse’. Berikut adalah tampilan yang muncul untuk mencari file



Gambar 9. Tampilan pencarian file pesan

Pesan yang digunakan kemudian ditentukan jumlah karakternya, agar user mengetahui jumlah karakter kunci yang harus diinputkan. Pada *algoritma One Time Pad*, jumlah karakter kunci harus sama dengan plainteks. Oleh karena itu, pada aplikasi akan muncul peringatan jika jumlah karakter kunci yang diinput user tidak sama dengan plainteks,seperti terlihat pada gambar 10.



Gambar 10. Tampilan *Error Message*

Gambar 11 berikut adalah contoh tampilan form enkripsi yang telah diinput nilainya dan dijalankan oleh user.

Gambar 11. Tampilan proses Enkripsi

Cipherteks yang dihasilkan kemudian disimpan dan pada implementasinya pesan inilah yang dikirimkan kepada penerima pesan. *Algoritma One Time Pad*, sebagaimana telah disebutkan sebelumnya, termasuk ke dalam algoritma kunci simetris dimana kunci enkripsi sama dengan kunci dekripsi. Oleh karena itu, selain cipherteks, pengirim juga harus mengirimkan kunci kepada penerima agar proses dekripsi bisa dijalankan. Proses dekripsi ditunjukkan pada gambar 12 berikut.

Gambar 12. Tampilan Proses Dekripsi

Berdasarkan penerapan *algoritma One Time Pad* di atas diketahui bahwa algoritma ini cukup untuk memenuhi aspek kerahasiaan sebagai salah satu tujuan diterapkannya algoritma kriptografi. Hal ini disebabkan pesan yang telah dienkripsi berubah menjadi pesan lain yang tidak dapat langsung dimengerti oleh penyadap karena bentuknya sudah tidak lagi sama dengan pesan asli. Algoritma ini juga masih cukup aman sebab kunci yang digunakan untuk setiap karakter hanya digunakan dalam satu kali proses enkripsi.

Hanya saja, penerapan algoritma ini memunculkan masalah distribusi kunci, dimana kunci harus dikirimkan melalui media yang benar-benar aman dari penyadapan dan tidak boleh menggunakan media pengiriman yang sama dengan pengiriman cipherteks. Sebab jika media tersebut disadap, penyadap langsung memiliki keduanya, baik cipherteks dan kunci, sehingga sangat mudah baginya untuk melakukan proses dekripsi dengan menggunakan persamaan dekripsi.

4. KESIMPULAN

Berdasarkan pembahasan yang telah dilakukan, maka kesimpulan yang diperoleh adalah :

1. *Algoritma One Time Pad* merupakan algoritma yang sederhana namun sangat aman karena kunci hanya digunakan satu kali dan setelah itu.
2. Dibutuhkan kunci yang sama panjang dengan plainteks sehingga semakin panjang plainteks semakin panjang kunci.

DAFTAR PUSTAKA

Amin., Miftakhul. M., 2014. ,*Image Steganography* dengan metode *Least Significant Bit*(LSB),CSRID Journal,Volume 6.

Connelly, Jeff., 2008, *"A Practical Implementation of a One-time Pad Cryptosystem"*, CPE 456.

Muliono, Hengky., & Rodiah, 2013. *Implementasi Algoritma One Time Pad pada Penyimpanan Data Berbasis Web*, Seminar Nasional Teknologi Informasi dan Multimedia ,Yogyakarta

Nurhayati ,2013, Analisis Kriptografi dengan Metode Hill *Cipher* , *Seminar Nasional Informatika,* Medan

Patil, Shared & Kumar, Ajay., 2002. *Effective Secure Encryption Scheme [One Time Pad] Using Complement Approach*, International Journal of Computer Science and Security (IJCSS), Volume (3) : Issue (2)

Pratiwi, Lis Endah., Marwatie, Rini., & Yusnitha, Isnie., 2014. *Program Aplikasi Kriptografi Penyandian One Time Pad Menggunakan Sandi Vigenere*, Jurnal Eureka Matika, No. 1 Vol. 1.