IMPLEMENTASI APLIKASI PENGAMANAN PESAN GAMBAR MENGGUNAKAN ALGORITMA ONE TIME PAD

Angga Aditya Permana [1], Rohmat Taufiq [2], Rachmat Destriana [3]
[1,2,3] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Tangerang
e-mail: [1]anggapermana@ft-umt.ac.id, [2] rohmat.taufiq@umt.ac.id, [3]rachmat.destriana@ft-umt.ac.id

ABSTRAK

Teknik pengamanan / kriptografi sudah sangat berkembang seiring perkembangan zaman. Yang tadinya hanya dapat dilakukan di media kertas sekarang sudah merambah ke dunia digital, dan juga semakin banyak variasi nya walaupun tujuannya masih sama yaitu mengamankan data agar tidak dapat diketahui dari orang yang tidak bertanggung jawab. Contohnya pada saat transaksi online transaksi-transaksi yang terjadi diamankan oleh enkripsi agar tidak dapat terlihat dengan kasat mata oleh para "Intruder". Pada penelitian ini menggunakan algoritma One-Time-Pad (OTP). Algoritma OTP adalah algoritma yang sangat baik tidak bisa dipecahkan tetapi algoritma OTP memiliki kelemahan dalam menjaga kerahasiaan atau keamanan kunci sehingga harus diberikan pengamanan pada kunci agar kunci dari OTP itu selama pengiriman terjaga kerahasiaanya. OTP merupakan algoritma klasik simetris yang dapat mengenkripsi sebuah pesan rahasia berupa gambar, algoritma ini tergolong sebagai algoritma yang sempurna dan sulit dipecahkan, karena setiap kunci yang dipakai tidak akan dapat dipakai lagi oleh karena itu lah disebut One-Time-Pad. Aplikasi pengamanan pesan menggunakan algoritma One-Time-Pad telah berhasil diterapkan pada media gambar menggunakan pemrograman java dan telah di uji coba menggunakan pendekatan blackbox testing.

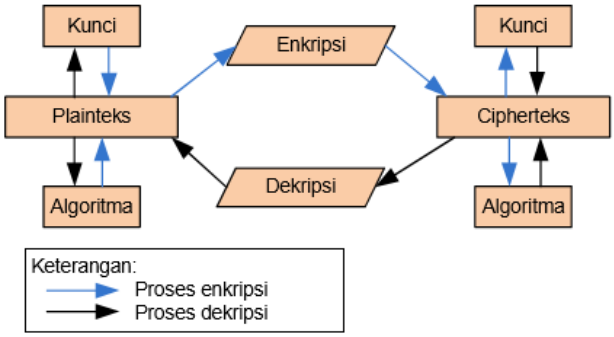
***Kata Kunci**: Kriptografi, One Time Pad, gambar.*

1. PENDAHULUAN

Pertumbuhan penggunaan media digital semakin tahun semakin bertambah, ada yang memanfaatkannya untuk pendidikan, kesehatan, hiburan dan lain-lain. Banyaknya pertukaran informasi yang beredar di dunia maya atau dunia digital menjadi perhatian khusus, apalagi jika informasi yang di kirim melalui dunia maya atau dunia digital tersebut merupakan informasi yang harus dijaga kerahasiaannya, agar tidak di salah gunakan oleh orang yang tidak bertanggung jawab.

Menjaga sebuah informasi menjadi sangat penting untuk dilakukan agar data yang bertukar di dunia maya atau dunia digital menjadi lebih aman, karena belum tentu penyedia jasa internet tersebut memberikan jaminan khusus untuk setiap data yang bertukar pada dunia maya atau dunia digital, data yang dikirimkan bisa berupa data teks, data gambar, data audio ataupun data video. Algoritma OTP adalah algoritma yang sangat baik tidak bisa dipecahkan tetapi algoritma OTP memiliki kelemahan dalam menjaga kerahasiaan atau keamanan kunci sehingga harus diberikan pengamanan pada kunci agar kunci dari OTP itu selama pengiriman terjaga kerahasiaanya [1].

Teknik penyembunyian data yang bertujuan untuk mengamankan keamanan dari data tersebut sudah sangat dikenal di khalayak masyarakat. Teknik-teknik yang tersebut dikenal dengan kriptografi , kriptografi merupakan ilmu utuk mengamankan data dalam operasi penyandian pada algoritma tertentu [2], dimana teknik ini sudah ada sejak romawi kuno. Kriptografi tradisional digunakan untuk mengamankan atau menyandikan informasi pada saat masa perang agar musuh tidak dapat mengambil informasi yang dapat menguntungkan pihak lawan. Namun seiring berkemabangnya zaman teknik kriptografi ini telah di kembangkan sampai tahap penyandian digital yang dapat di proses oleh komputer yang tujuannya sama untuk mengamankan kemanan dari serangan luar.



Gambar 1. Alur kerja teknik kriptografi [3]

Kriptografi

Kriptografi adalah ilmu mengenai teknik enkripsi dimana "naskah asli" (*plaintext*) diacak menggunakan suatu kunci enkripsi menjadi "naskah acak yang sulit dibaca" (*ciphertext*) oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi dalam waktu yang tidak terlalu lama adalah sangat kecil. Teknik enkripsi yang digunakan dalam kriptografi klasik adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk *public key cryptography*, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan – bilangan yang sangat besar. [4]

Algoritma One Time Pad (OTP)

One Time Pad merupakan salah satu algoritma yang populer dan sering digunakan dalam teknik kriptografi. OTP termasuk kelompok algoritma yang simetris dalam kriptografi dimana kunci enkripsi dan dekripsi dalam bentuk dan panjang yang sama, serta menggunakan operasi XOR [3]. Keunggulan OTP adalah sangat sulit untuk dipecahkan tapi memiliki kekurangan dimana kunci yang digunakan kadang terlalu panjang karena harus menyesuaikan jumlah karakter yang akan dienkripsi [5]. Dari semua metode kriptografi yang telah "Sempurna" dirancang, OTP adalah metode yang telah terbukti benar-benar aman secara matematis.*One Time Pad* bisa dikatakan jika memenuhi kondisi berikut [6] kunci harus sepanjang plainteks, kunci harus acak seluruhnya atau sepenuhnya berbeda, kunci hanya sekali digunakan setiap melakukan enkripsi, danhanya terdapat dua salinan dari kunci: satu untuk pengirim dan satu untuk penerima [7] Rumus enkripsi dan dekripsi OTP dalam dijabarkan melalui Persamaan 1 dan Persamaan 2.

$$Cc = (Cc-k) \bmod X$$

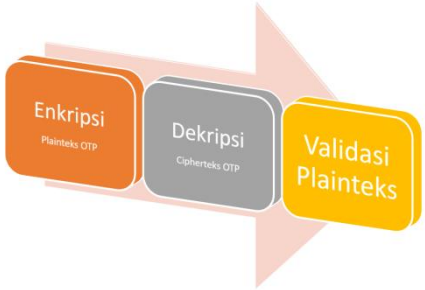
dimana: Cc = Citra cipher, Ca = Citra asli, k = kunci random. X = nilai maksimal intensitas citra Sedangkan untuk melakukan dekripsi menggunakan rumus:

$$Cc = (Ca+k) \bmod X$$

Semakin banyaknya pertukaran informasi yang terjadi pada saat ini, maka banyak orang yang menginginkan informasi tersebut untuk bisa di manfaatkan bagi kepentingan pribadi maupun kelompok atau golongan tertentu. Kasus tersebut bisa terjadi jika tidak adanya sebuah teknik keamanan yang baik dari pertukaran informasi yang penting. Berdasarkan masalah yang ada, maka pengamanan informasi sangatlah penting untuk di lakukan agar informasi yang bersifat rahasia dapat di amankan dan tidak bisa di ambil oleh pihak yang tidak berwenang. Maka aplikasi yang akan dibuat adalah sebuah aplikasi pengamanan data berupa gambar yang berfungsi melindungi informasi dari pihak yang tidak bertanggung jawab. Oleh karena itu diperlukan sebuah aplikasi pengamanan data gambar, dalam hal ini pengamanan data gambar dilakukan dengan menggunakan teknik kriptografi menggunakan algoritma *One Time Pad* berbasis *Java.*

2. METODE PENELITIAN

Metode yang dilakukan pada penelitian ini terdiri dari 3 tahapan, seperti yang di tunjukkan pada gambar 2.



Gambar 2. Metode Penelitian Analisa Algoritma OTP

Pesan asli atau plainteks disandikan (*enkripsi)* dengan menggunakan algoritma OTP. Sebelum proses *enkripsi* dilakukan, terlebih dahulu dilakukan pembangkitan bilangan acak yang akan digunakan sebagai *key.*

Panjang bilangan acak yang akan digunakan haru sama panjangnya dengan *plainteks* atau pesan asli yang akan *enkripsi*.

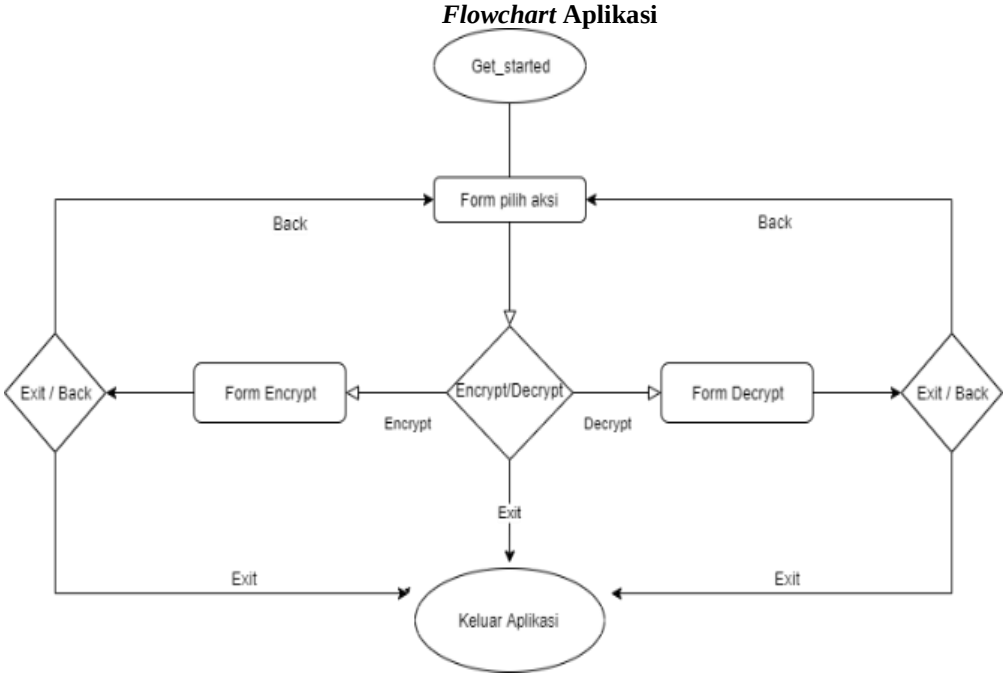
Pesan yang sudah atau telah di*enkripsi* disebut dengan *cipherteks* kemudian didekripsi kembali untuk mengembalikan pesan asli (*plainteks).* Pada implementasinya, proses *dekripsi* dilakukan oleh penerima pesan rahasia agar pesan yang diterima dapat dipahami.

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

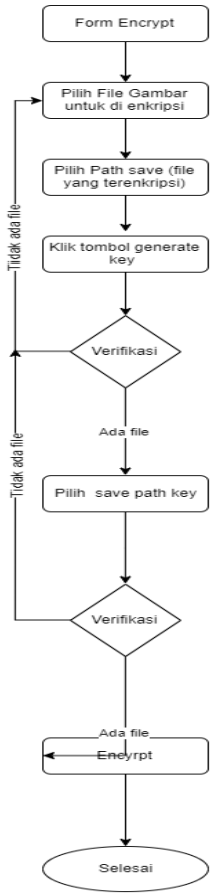
3. HASIL DAN PEMBAHASAN

Dalam penelitian ini, penulis mencoba merancang sebuah aplikasi pengamanan data gambar menggunakan algoritma *One Time Pad.* Dengan menggunakan algoritma ini diharapan penulis dapat mengembangkan sebuah aplikasi pengamanan data gambar yang memungkinkan pengguna untuk mengenkripsi data gambar dengan algoritma *One Time Pad.* Aplikasi pengamanan ini dibuat menggunakan bahasa JAVA. Berikut ini adalah *flowchart, User Interface* dan Hasil pengujian menggunakan *Black Box Testing.*

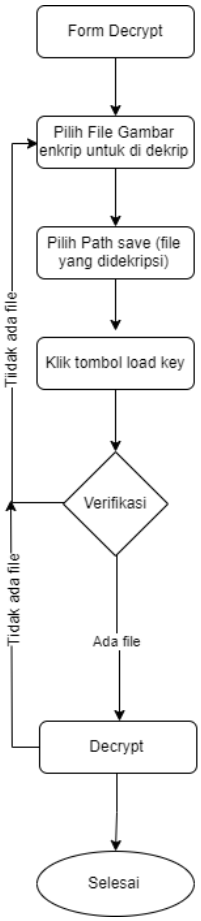
***Flowchart* Aplikasi**



Gambar 3. *Flowchart* menu utama



Gambar 4. *Flowchart* Menu En*crypt*



Gambar 5. *Flowchart* Menu *Decrypt*

User Interface

- Halaman Utama

Gambar 6. *User Interface* Halaman Utama

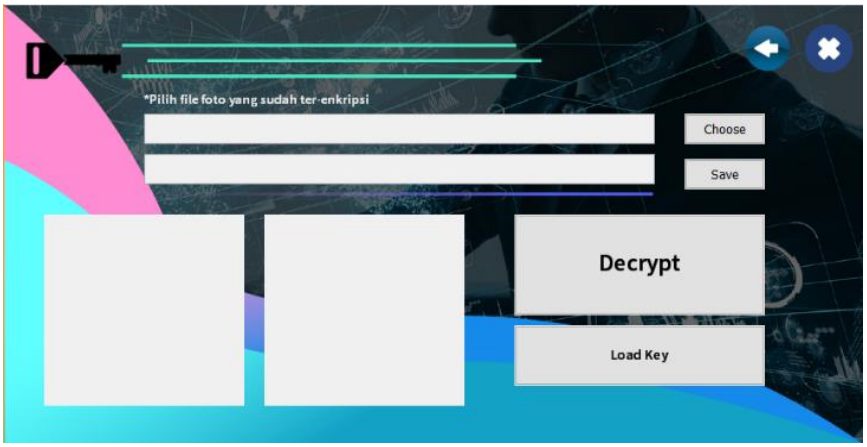
- Pilih Aksi

Gambar 7. *User Interface* Menu Utama

- Menu Enkrip

Gambar 8. *User Interface* Menu Enkrip

- Menu Dekrip

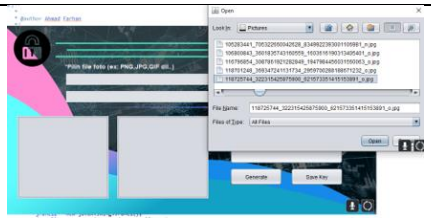
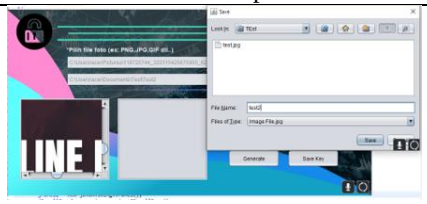
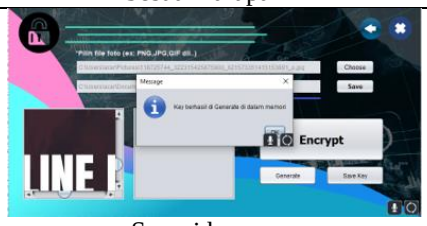
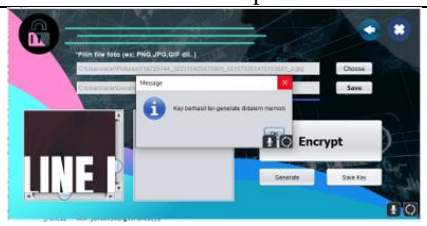


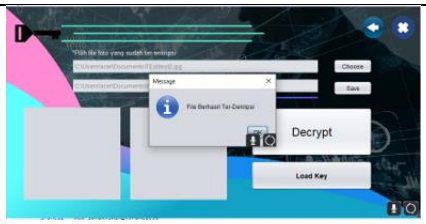
Gambar 9. *User Interface* Menu

Hasil *Black Box Testing*

Pada aplikasi ini penulis melakukan pendekatan yang dilakukan dengan menguij secara fungsioalitas dari fungsi sistem, apakah sistem berfungsi dengan hasil yang sesuai dengan skenario atau tidak. Pada aplikasi pengamanan pesan gambar menggunakan algoritma *one time pad* ini, melakukan pengujian dengan pendekatan yang merujuk pada fungsi – fungsi yang dimiliki sistem, kemudian dibandingkan antara hasil yang diharapkan dengan hasil pengujian. Jika hasil yang diharapkan sesuai dengan hasil pengujian maka aplikasi sesuai dengan desain yang telah di tentukan sebelumnya. Tetapi bila belum sesuai antara hasil yang diharapkan dengan hasil pengujian maka perlu adanya dilakukan pengecekan lebih lanjut dan setelah itu dilakukan perbaikan agar hasil yang diharapkan sesuai dengan hasil pengujian. Berikut ini adalah hasil pengujian menggunakan pendekatan *black box testing* yang di tampilkan pada tabel 1.

Tabel 1. Hasil Uji Coba Aplikasi

No	Skenario Pengujian	*Test Case*	Hasil yang diharapkan	Hasil pengujian	Simpulan
1	Mengambil file dari directory yang tersedia	*Choose*	Sistem akan meng save dan mewrite directory yang tersedia ke text field Choosepath	 Sesuai harapan	*Valid*
2	Menyimpan file yang akan di enkripsi	*Save*	Sistem akan meng save dan mewrite directory yang tersedia ke text field Save Path	 Sesuai harapan	*Valid*
3	Meng Generate key dari file yang sudah di input	*Generate*	Sistem akan membuat key dari file dengan panjang bit yang sama dengan bit dari si file dan menyimpannya ke memory	 Sesuai harapan	*Valid*
4	*Save key* kedalam *directory* yag diinginkan	*Save Key*	Sistem akan meng save key yang sudah di generate didalam memory dan menyimpan ke path yang diinginkan	 Sesuai harapan	*Valid*
5	Enkripsi file yang sudah di *input*	*Save*	Sistem akan meng save dan mewrite directory yang tersedia ke text field Save Path	 Sesuai harapan Namun dalam beberapa gambar terdapat bug yang membuat ¼ gambar hilang setelah di dekripsi	*Valid*

6	Mengdekripsi kan file yang sudah ter enkripsi	*Decrypt*	Sistem akan mengdecrypt file yang telah di input kan sebelumnya dengan key yang sudah di load terlebih dahulu	 Sesuai harapan	*Valid*

5. KESIMPULAN

Setelah menganalisis dan mengimplementasikan aplikasi pengamanan pesan gambar menggunakan algoritma *One-Time-Pad* telah berhasil diterapkan menggunakan pemrograman *java*, walaupun data yang diberikan belum sepenuhnya *random* karena masih melakukan *generate* menggunakan *Pseudo Random Key* dalam pemrosesan *Generate Key* nya akan menyamai jumlah bit dengan panjang bit pada gambar itu sendiri.

DAFTAR PUSTAKA

[1] M. Stamp, 2011. Information Security, 2nd Edition. John Wiley & Sons Inc: New York.
[2] R. Munir. 2011. Algoritma dan Pemrograman. Bandung : Informatika
[3] D.R.I.M. Setiadi, E.H. Rachmawanto, C.A Sari. 2017. Implementasi One Time Pad Kriptografi pada Gambar Grayscale dan Gambar Berwarna. Prosiding Seminar Nasional Multi Disiplin Ilmu & Call for Papers Unisbank Ke-3 (SENDI-U 3) 2017 ISBN: 9-789-7936-499-93
[4] S. Kromodimoeljo. 2010. Teori dan Aplikasi Kriptografi. SPK IT Consulting: Jakarta.
[5] O. Tornea, et al., 2011. DNA Vernam Cipher. Proceedings of the 3rd International Conference on E-Health and Bioengineering - EHB 2011, pp.24 27.
[6] E.H. Rachmawanto & C.A Sari., 2015. Keamanan File Menggunakan Teknik Kriptografi Shift Cipher. Techno.COM, 14(4), pp.329 335
[7] R. Shukla, et al., 2013. Sampurna Suraksha: Unconditionally Secure and Authenticated One Time Pad Cryptosystem. In 2013 International Conference on Machine Intelligence and Research Advancement. IEEE, pp. 174 178