RANCANG BANGUN APLIKASI KEAMANAN DATA TEKS MENGGUNAKAN ALGORITMA STREAM CIPHER

Design Of Text Data Security Applications Using Stream Cipher Algorithm

Aris Munandar[1], Rika Rosnelly[2] , Charles Jhony Mantho Sianturi [3]
[1]Jurusan Teknik InformatikaUniversitas Potensi Utama
[2,3]Dosen Jurusan Teknik InformatikaUniversitas Potensi Utama
[1,2,3]Universitas Potensi Utama, K.L. Yos Sudarso KM 6,5 No. 3A Tj. Mulia - Medan
Email : [1]arismunandarsyarif@gmail.com, [2]rikarosnelly@gmail.com, [3]lapetgadong@yahoo.com

ABSTRAK

Pada zaman ini perkembangan teknologi informasi sangat canggih sekali dalam kehidupan kita sehari – hari, misalnya dalam pencaharian informasi – informasi di seluruh dunia dapat kita ketahui sesuai keinginan. Dengan demikian untuk mendapatkan suatu data seharusnya dapat menjaga kerahasiaan dari sumber data tersebut dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna informasi, karena informasi merupakan suatu data yang sangat penting dalam kehidupan sehari – hari. Oleh karena itu pengamanan bisa dilakukan dengan banyak cara, mulai dari penggunaan algoritma yang sederhana hingga kompleks seperti algoritma stream cipher. Dengan enkripsi menggunakan Stream Cipher tentunya data menjadi lebih aman dan terjaga keasliannya. Penelitian ini secara khusus membahas tentang bagaimana mengenkripsi dan mendekripsi sebuah file teks, dimana setiap digit plaintext dienkripsi satu persatu dengan digit yang sama dari keystream, untuk memberikan digit dari aliran ciphertext. Karena enkripsi setiap digit bergantung pada status cipher saat ini, ia juga dikenal sebagai cipher status. Berdasarkan hasi pengujian pada penelitian yang dilakukan bahwa algoritma Stream Cipher menggunakan kunci simetrik di mana digit plaintext digabungkan dengan aliran digit cipher pseudorandom (keystream).

Kata Kunci : Aplikasi, Enkripsi, Metode Stream Cipher, File Teks.

ABSTRACT

At this time the development of information technology is very sophisticated in our daily lives, for example in the search for information - information throughout the world can we know as you wish. Thus, to obtain data, it should be able to maintain the confidentiality of the data source by disguising it into a encrypted form that has no information meaning, because information is a data that is very important in daily life. Therefore, security can be done in many ways, ranging from the use of simple to complex algorithms such as the stream cipher algorithm. With encryption using the Stream Cipher of course the data becomes more secure and maintained its authenticity. This research specifically discusses how to encrypt and decrypt a text file, where each digit of the plaintext is encrypted one by one with the same digits of the keystream, to provide digits from the ciphertext stream. Because encryption of each digit depends on the current cipher status, it is also known as the cipher status. Based on the results of tests on research conducted that the Stream Cipher algorithm uses a symmetric key in which the plaintext digits are combined with the pseudorandom digit cipher flow (keystream).

Keywords : Applications, Encryption, Stream Cipher Methods, Text Files.

1. PENDAHULUAN

Pertukaran suatu informasi dalam kehidupan kita dengan orang lain dimanapun kita berada merupakan salah satu cara yang lebih baik secara efektif dan efesien, sehingga sangat mudah untuk mendapatkan suatu informasi tersebut. Ada banyak cara yang bisa dilakukan untuk mendapatkan suatu informasi yang sesuai dengan keingininan, misalnya melalui teknologi secara langsung maupun secara tidak langsung. Di dalam informasi juga banyak hal-hal yang bisa membangun sesuatu yang baru. Masalah keamanan dan kerahasiaan suatu data tersebut merupakan salah satu aspek penting dari suatu inforrnasi.

Stream cipher adalah jenis algoritma enkripsi simetri, yaitu kunci pada saat mengenkripsi sama dengan kunci pada saat mendekripsi. Stream cipher dapat dibuat dengan cepat bahkan lebih cepat dibandingkan dengan algoritma block cipher manapun. Algoritma block cipher secara umum digunakan untuk blok data yang besar sedangkan stream cipher digunakan untuk blok data yang lebih kecil, biasanya ukuran bit. Proses enkripsi terhadap plaintext dengan algoritma block cipher akan menghasilkan ciphertext yang sama [1].

Berdasarkan penelitian mengenai "Pengembangan Aplikasi Kriptografi Berbasis *Bit Inserted Carrier* (BIC)*".* penelitian ini menghasilkan sebuah aplikasi yang dibangun dapat mengukur kualitas kunci yang di-*input* dan dapat memeriksa valid- asi kunci ketika proses dekripsi dilakukan [2].

Berdasarkan penelitian mengenai "Implementasi Sistem Sandi *Stream Cipher* Untuk Pengamanan Data *Image*", Setyaningsih menyimpulkan bahwa Algoritma enkripsi pada *image* yang diusulkan cukup efektif karena proses enkripsi maupun pada *image* tidak membutuhkan waktu yang lama [3].

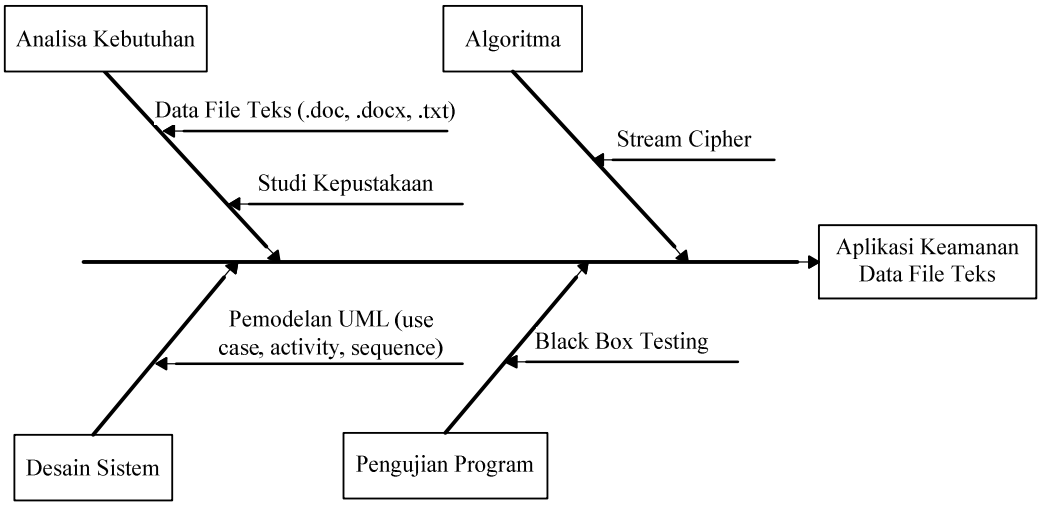
Berdasarkan penelitian yang berjudul "Implementasi Teknik Kriptografi *Stream Cipher* Salsa20 Untuk Pengamanan Basis Data*".* Penelitian ini menyimpulkan bahwa teknik kriptografi *stream cipher* Salsa20 dapat digunakan untuk memberikan peningkatan keamanan data melalui proses enkripsi-dekripsi sebelum data disimpan di dalam sebuah basis data [4].

Teknik Kriptografi dengan metode Algorita *Stream Cipher* dapat diterapkan untuk menjamin keamanan *file* dokumen *elektronis.* Salah satu yang dapat dimanfaatkan adalah enkripsi dan dekripsi data teks atau dengan kata lain menyandikan data sehingga hanya orang yang dimaksud saja yang dapat mengetahui isi data tersebut.

Berdasarkan dari beberapa penelitian di atas maka tidak ditemukan adanya kesamaan judul dan sistem yang di bahas, oleh karena itu referensi dari kedua penelitian di atas dapat digunakan sebagai referensi untuk penelitian ini.

2. METODE PENELITIAN

Metode merupakan cara yang sistematik untuk mengerjakan/memecahkan suatu permasalahan. Penelitian ini akan melalui beberapa tahapan. Tahapan yang dilakukan dalam penelitian ini dimodelkan pada diagram *Fish bone*. Adapun beberapa tahapan yang digunakan dalam penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. Diagram *Fish Bone*

Pada tampilan diagram *fish bone* pada Gambar 1. terlihat proses-proses atau tahapan metodologi penelitian yang dibuat. Adapun tahapan – tahapan metodologi penelitian pada pembuatan aplikasi ini meliputi :

1. Analisa Kebutuhan

   Dalam tahap ini dilakukan proses pencariaan bahan-bahan yang berkaitan dengan perancangan aplikasi enkripsi keamanan data teks menggunakan algoritma *stream cipher* pada perangkat desktop. Pengutipan yang dilakukan berupa teori ataupun berbagai pendapat dari beberapa buku bacaan, jurnal maupun buku diktat yang dipergunakan selama kuliah untuk menunjang perancangan program aplikasi.

2. Desain Sistem

   Secara umum Rancang Bangun Aplikasi Keamanan Data Teks dengan Algotirma *Stream Cipher* menggunakan model perancangan *Unified Modelling Language* yang meliputi *usecase diagram, activity diagram,* dan *sequence diagram* . Pada tahap ini akan dilakukan perancangan pada aplikasi yang akan dibuat meliputi model sistem, perancangan arsitektural dan perancangan antarmuka.

3. Algoritma

   Perancangan aplikasi ini menggunakan algoritma pemrograman yaitu *stream cipher*. *Stream cipher* merupakan algoritma yang mirip dengan *caesar cipher* (*cipher* yang menggeser urutan alphabet sehingga urutan alfabetnya berubah), tetapi *cipher* ini mempunyai kunci yang unik, yaitu menggunakan karakter sebelumnya sebagai kunci [5].

4. Pengujian Program

   Pada tahap ini akan dilakukan pengujian aplikasi secara menyeluruh, meliputi Pengujian secara teori menggunakan *blackbox testing* dan pengujian aplikasi menggunakan pemrograman VB NET 2010.

5. Hasil

   Pada tahapan ini merupakan hasil dari perancangan sistem, dan sistem yang telah dibuat berbentuk sebuah Aplikasi Keamanan Data Teks menggunakan Algoritma *Stream Cipher*.

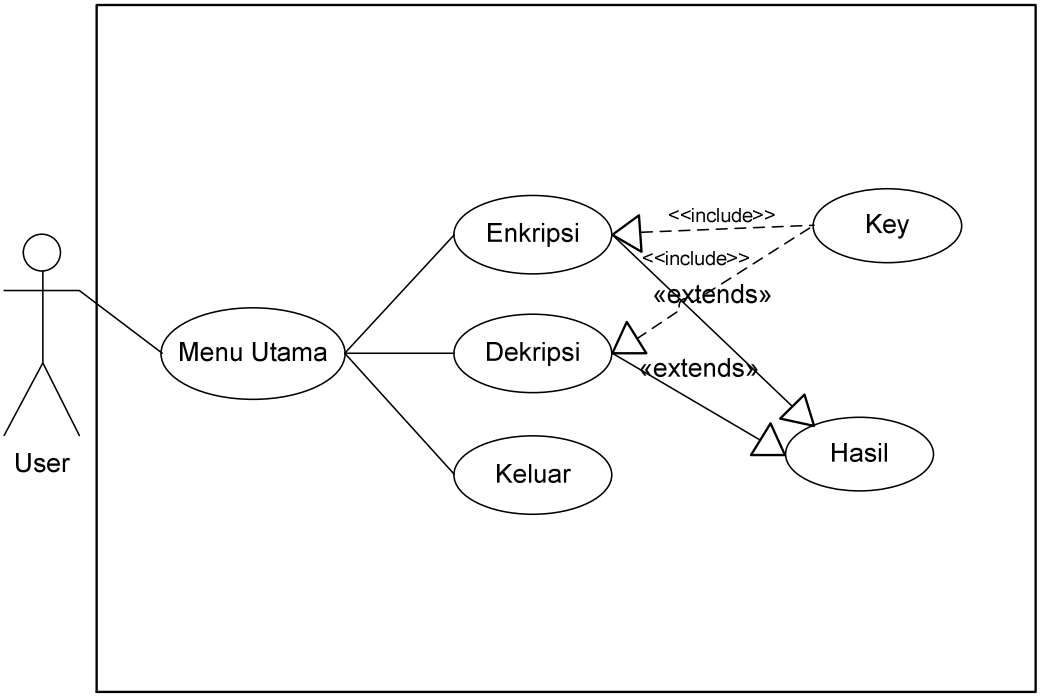
3. HASIL DAN PEMBAHASAN

3.1. Desain Sistem

Perancangan ini akan memberikan penjelasan mengenai rancangan aplikasi serta pembentukan dan pembangunan aplikasi kriptografi algoritma *Stream Cipher* dalam mengamankan data *file* teks. Bentuk perancangan sistem yang penulis buat menggunakan beberapa bentuk diagram dari *Unified Modeling Language* (UML) yaitu *Use Cace Diagram*, *Activity Diagram* dan *Sequence Diagram.*

3.1.1. *Use Case Diagram*

Secara umum *use case diagram* akan menampilkan tugas – tugas dari tiap elmen yang terlibat dalam sistem yang akan ditampilkan pada Gambar 2.



Gambar 2. *Usecase Diagram*

Pada tampilan *use case* diagram Gambar 2. terlihat proses-proses atau tahapan yang dilalui pada saat pengguna melakukan akses terhadap aplikasi, berikut adalah tahapan yang akan dilalui oleh pengguna aplikasi :

1. Menu Utama
   Pada menu utama terdapat sub menu enkripsi dekripsi dan keluar. Pengguna (*user)* memasuki menu utama dan memulai beberapa menu selanjutnya.
2. Menu Enkripsi dan Dekripsi

User memilih *button* "browse" pada menu enkripsi dan dekripsi untuk mengambil *file* yang akan dienkripsi, lalu *user* memasukkan *key* sehingga proses enkripsi bisa dilakukan dengan menekan tombol enkripsi dan dekripsi.

3. Tentang
   User memilih tombol tentang, maka *user* dapat membaca informasi pembuat aplikasi.
4. Keluar
   User dapat menekan tombol keluar untuk keluar dari aplikasi.

3.2. Hasil

Berikut ini akan dijelaskan tentang tampilan hasil dari Aplikasi Keamanan Data Teks Menggunakan Algoritma *Stream Cipher*.

3.2.1.Tampilan *Form* Menu Utama

Berikut ini merupakan tampilan *form* menu dapat dilihat pada Gambar 3.

Gambar 3. Tampilan *Form* Menu Utama

Pada tampilan Gambar 3 ini terdapat *menu* utama aplikasi enkripsi dan dekripsi stream cipher, pada bagian sub menu terdapat menu – menu lainnya seperti menu *file* dan menu keluar. Pada menu file terdapat sub menu enkripsi dan dekripsi, dan menu keluar berfungsi untuk mengakhiri dari aplikasi ini.

3.2.2. Tampilan *Form* Enkripsi dan Dekripsi

Berikut ini merupakan tampilan *form* enkripsi dan dekripsi dapat dilihat pada Gambar 4.

Gambar 4. Tampilan *Form* Enkripsi dan Dekripsi

Pada tampilan Gambar 4 ini terdapat *menu* utama aplikasi enkripsi dan dekripsi stream cipher, pada bagian sub menu terdapat menu – menu lainnya seperti about untuk menampilkan tentang aplikasi dan penulis, dan menu keluar berfungsi untuk mengakhiri dari aplikasi ini.

3.2.3. Tampilan *Form About*

Berikut ini merupakan tampilan *form about* dapat dilihat pada Gambar 5.

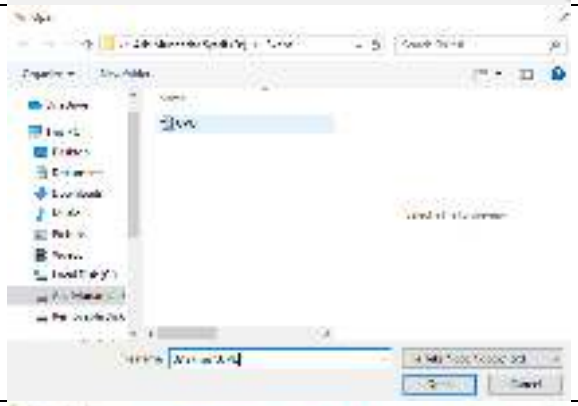
Gambar 5. Tampilan *Form About*

Pada tampilan Gambar 5 menampilkan form about yang berisi tentang aplikasi dan profil penulis.

3.3. Uji Coba Program

Adapun skenario pengujian program aplikasi yang dilakukan ialah dengan menggunakan metode pengujian aplikasi berupa *Blackbox Testing* :

Tabel 1. *Blackbox Testing Form* Menu Utama & *Form* Enkripsi

No	Tes *Case*	Keterangan	Hasil Pengujian	Hasil
1.	Klik *File*	Sistem akan menampilkan menu pilihan *file.*		*Valid*
3.	Klik Enkripsi dan Dekripsi	Sistem akan menampilkan *form* enkripsi dan dekripsi.		*Valid*
4.	Klik *Browse*	Sistem akan menampilkan menu untuk mengambil *file.*		*Valid*
5.	Klik Enkripsi	Sistem akan mengenkripsi *file.*		*Valid*

8.	Klik Dekripsi	Sistem akan mendekripsi *file.*		*Valid*
2.	Klik *About*	Sistem akan menampilkan menu pilihan *about.*		*Valid*
9.	Klik Keluar	Sistem akan menutup semua *form*.	-	*Valid*

3.4. Hasil Uji Coba

Setelah melakukan uji coba, maka dapat disimpulkan hasil yang didapatkan yaitu :

1. Metode berhasil diterapkan ke sistem.
2. Aplikasi telah sesuai dengan rancangan.
3. Proses enkripsi dan dekripsi telah sesuai.
4. Penggunaan aplikasi yang tidak sulit.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan selama membuat aplikasi ini, maka dapat ditarik beberapa kesimpulan sebagai berikut:

1. Dengan menggunakan *Visual Basic* 2010 maka dapat menghasilkan aplikasi penyandian data teks menggunakan metode *stream cipher*.
2. Metode *stream cipher* dapat merubah *file* teks asli menjadi *file* teks sandi dengan perhitungan yang mengkonfersikan *file* asli dengan kunci.
3. Aplikasi enkripsi *file* teks menggunakan metode *stream cipher* dapat diuji berulang kali dan mendapatkan hasil yang baik.

5. SARAN

Sebagai aplikasi yang tidak dikerjakan dengan tim, penulis menyadari bahwa aplikasi ini memiliki banyak kekurangan, saran untuk pengembangan aplikasi pada waktu mendatang adalah :

1. Melakukan pengembangan aplikasi *file* teks dengan menambahkan *file* yang bisa dienkripsi dan didekripsi seperti, gambar, video, audio, dan *file – file* lainnya.

2. Aplikasi enkripsi *file* teks menggunakan metode *stream cipher* dapat menggunakan metode lain yang penyandiannya lebih kuat.
3. Aplikasi enkripsi *file* teks menggunakan metode *stream cipher* dapat diterapkan pada perangkat *mobile*.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Universitas Potensi Utama yang telah mebantu penulis dalam menyelesaikan laporan penelitian ini.

DAFTAR PUSTAKA

[1] https://dimasandree.wordpress.com/2013/11/18/stream-cipher/
[2] Triandi, B. PENGEMBANGAN APLIKASI KRIPTOGRAFI BERBASIS BIT INSERTED CARRIER (BIC).
[3] Setyaningsih, Emy, 2013, "Implementasi System Sandi Stream Cipher Untuk Pengamanan Data Image." Seminar Nasional Teknologi Informasi dan Komputasi 2013 (SENASTIK 2013), AKPRIND Yogyakarta, ISSN: 2302 – 7088.
[4] Irawan, Paulus Lucky Tirma, 2015, "Implementasi Teknik Kriptografi Stream Cipher Salsa20 Untuk Pengamanan Basis Data." SMATIKA JURNAL, Universitas Ma Chung, Malang, Vol 5.02, ISSN: 2087-0256.
[5] Nurwiyati dan Yatini B, 2013, Jurnal : "Enkripsi Dekripsi Data Menggunakan Metode Stream *Dan Vigenere Cipher*", STMIK AKAKOM Yogyakarta, Vol. 3, No. 23.
[6] Adhar, D. (2019). Implementasi Algoritma DES (Data Encryption Standard) Pada Enkripsi Dan Deskripsi SMS Berbasis Android. Jurnal Teknik Informatika Kaputama, 3(2).
[7] Zulham, M., Kurniawan, H., & Rahmad, I. F. (2017, October). Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi RC6 Berbasis Android. In Seminar Nasional Informatika (SNIf) (Vol. 1, No. 1, pp. 96-101).
[8] Sembiring, N. S. B. (2018). Perancangan Aplikasi Kriptografi Dengan Metode Modifikasi Caesar Cipher Yang Diperkuat Dengan Vernam Cipher Untuk Keamanan Teks. JUSITI: Jurnal Sistem Informasi dan Teknologi Informasi, 5(1), 10-17.
[9] Putra, D. I., & Ginting, G. (2017). Perancangan Aplikasi Penyandian Data Text Menggunakan Metode Symmetric Stream Cipher. Pelita Informatika: Informasi dan Informatika, 16(3).
[10] Setiawan, A. (2015). Perancangan Aplikasi Steganografi Dengan Algoritma Caesar Cipher Dan Pixel Value Differencing.
[11] Puspita, K., & Wayahdi, M. R. (2015, February). Analisis Kombinasi Metode Caesar Cipher, Vernam Cipher, Dan Hill Cipher Dalam Proses Kriptografi. In Jurnal Seminar Nasional Teknologi Informasi dan Multimedia.
[12] Sinaga, M. D., Sembiring, N. S. B., Tambunan, F., & Sianturi, C. J. M. (2018, August). Hybrid Cryptography WAKE (Word Auto Key Encryption) and Binary Caesar Cipher Method For Data Security. In 2018 6th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-5). IEEE.
[13] Adhar, D. (2017, October). Pengamanan SQLITE Database Menggunakan Kriptografi Elgamal. In *Seminar Nasional Informatika (SNIf)* (Vol. 1, No. 1, pp. 432-437).
[14] Khairani, S., Agustin, F., & Fahmi, A. Rancang Bangun Program Kriptografi Advanced Encryption Standard. *Creative Communication and Innovative Technology Journal*, *2*(3), 336-353.
[15] Nugroho, A. Y. (2017, November). PEMBUATAN APLIKASI KRIPTOGRAFI ALGORITMA BASE 64 MENGGUNAKAN PHP UNTUK MENGAMANKAN DATA TEXT. In *Seminar Nasional Informatika (SNIf)* (Vol. 1, No. 1, pp. 134-139).
[16] Syahputri, N. (2019). RANCANG BANGUN APLIKASI KRIPTOGRAFI PENGAMANAN TRANSMISI DATA MULTIMEDIA MENGGUNAKAN

ALGORITMA DATA ENCRYPTION STANDARD (DES). MAJALAH ILMIAH METHODA, 9(2), 57-63.

[17] Haryanto, E. V. (2015). Penerapan Metode Adaptif Dalam Penyembunyian Pesan Pada Citra. Proceedings Konferensi Nasional Sistem dan Informatika (KNS&I).

[18] Rambe, M. R., Haryanto, E. V., & Setiawan, A. (2018). Aplikasi Pengamanan Data dan Disisipkan Pada Gambar dengan Algoritma RSA Dan Modified LSB Berbasis Android. Konferensi Nasional Sistem Informasi (KNSI) 2018.

[19] Triandi, B. (2017, October). APLIKSASI TES BILANGAN PRIMA MENGUNAKAN RABINMILLER, GCD, FAST EXPONENSIAL DAN FAKTORISASI PRIMA UNTUK DASAR MATEMATIS KRIPTOGRAFI. In Seminar Nasional Informatika (SNIf) (Vol. 1, No. 1, pp. 277-232).

[20] Yusfrizal, Y. (2016). Aplikasi Enkripsi Data Menggunakan Metode RSA dan PGP.