P-ISSN : 2580-4316
E-ISSN : 2654-8054 https://doi.org/10.37817/ikraith-informatika.v11i2

APLIKASI *FAST* (k, n)-*THRESHOLD SECRET SHARING SCHEME*

Samuel Josuabryan Sirait[1], **Swingly Purba**[2], **Melva Pangaribuan**[3]

Jurusan Teknik Informatika, ISTP Medan

Penulis: bryansirait2003@gmail.com

ABSTRAK

Sebuah skema *secret sharing* memperbolehkan sebuah rahasia untuk dibagikan kepada n partisipan sedemikian sehingga hanya k orang dari mereka yang dapat mengkonstruksi pesan kembali, tetapi sembarang (k – 1) tidak dapat memperoleh informasi apapun mengenai rahasia. Dalam literatur, dapat ditemukan berbagai skema *secret sharing* yang menerapkan berbagai macam teorema. Suatu skema *secret sharing* dikatakan ideal apabila *share* yang dihasilkan memiliki ukuran bit yang sama dengan ukuran bit rahasia. Skema *secret sharing* dari Shamir merupakan salah satu skema *secret sharing* yang ideal. Namun, kekurangan dari skema Shamir ini adalah memiliki proses komputasi yang banyak, terutama untuk proses *recovery*.

Untuk memperbaiki masalah tersebut, dari (*Kokusai Denshin Denwa Institute*) R&D (*Research and Development*) Laboratories, Inc., Jepang memperkenalkan yang cepat. Prosedur kerja dari skema ini terbagi menjadi dua bagian, yaitu proses distribusi dan *recovery*. Prosedur kerja dalam skema ini menggunakan operasi logika XOR dan algoritma eliminasi Gauss.

Penulisan tugas akhir ini akan memfokuskan pembahasan pada prosedur. Perangkat lunak hasil rancangan akan mampu

Kata Kunci : *Kriptografi, Secret Sharing, Threshold*

P-ISSN : 2580-4316
E-ISSN : 2654-8054
https://doi.org/10.37817/ikraith-informatika.v11i2

ABSTRACT

Scheme allows a secret to be distributed participants such that only while any group of participants. Various secret sharing schemes based on different literature. Considered ideal if the generated shares have the same as itself. one such ideal scheme. However, a drawback of Shamir's scheme is its high computational overhead, particularly during the recovery process.

To address this issue,.(Japan) introduced scheme's operation consists of two parts: the distribution process and the recovery process. It utilizes XOR logic operations and the Gaussian elimination algorithm.

This final project focuses on the operational procedures of this secret sharing scheme and implements it to perform secret distribution and recovery. The designed software is capable of executing both the distribution and recovery processes. Additionally, the software generates reports detailing the calculations performed during these processes.

Keywords: Cryptography, Secret Sharing, Threshold

P-ISSN : 2580-4316
E-ISSN : 2654-8054 https://doi.org/10.37817/ikraith-informatika.v11i2

PENDAHULUAN

Dalam kehidupan sehari-hari, sering ditemui persoalan penyimpanan rahasia digital. Agar data rahasia digital tersebut aman, maka harus dipecahkan sehingga orang mengetahui beberapa informasi mengenai data rahasia tersebut. Hal ini menerapkan protokol kriptografi *secret sharing*. Konsep pertama kali diperkenalkan oleh Shamir dan Blakley pada tahun 1979. Konsep yang dihasilkan dari rahasia s. yang masing-masing dipegang oleh partisipan menampilkan sehingga dapat

RUMUSAN MASALAH

Skema *secret sharing* yang diperkenalkan oleh para pengembang dari KDDI ini menerapkan operasi XOR pada proses distribusi serta konsep matriks dan eliminasi Gauss pada proses *recovery*. Berhubung karena banyaknya konsep yang diterapkan, maka diperlukan sebuah perangkat lunak pemahaman yang mampu untuk menunjukkan langkah kerjanya secara bertahap. Selain itu, untuk dapat mengimplementasikan skema *secret sharing* ini juga diperlukan sebuah aplikasi dari skema *secret sharing* tersebut.

BATASAN MASALAH

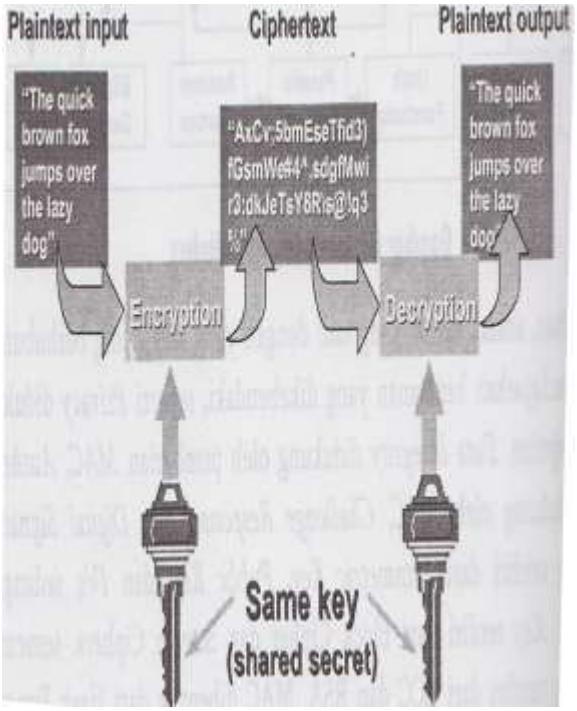
1. Nilai k dan n dibatasi maksimal 10, dimana $k \leq n$. (untuk pemahaman)
2. Nilai k dan n dibatasi maksimal 50, dimana $k \leq n$. (untuk penerapan)
3. Panjang pesan rahasia maksimal 50 karakter. (untuk pemahaman)
4. Panjang pesan rahasia maksimal 1000 karakter. (untuk penerapan)
5. Pembangkitan dan pengujian bilangan prima menggunakan metode Rabin-Miller dengan batasan minimal 1 digit dan maksimal 2 digit.

P-ISSN : 2580-4316
E-ISSN : 2654-8054
https://doi.org/10.37817/ikraith-informatika.v11i2

6. Perangkat lunak akan menampilkan laporan hasil proses perhitungan yang dapat disimpan dalam bentuk *text file*.

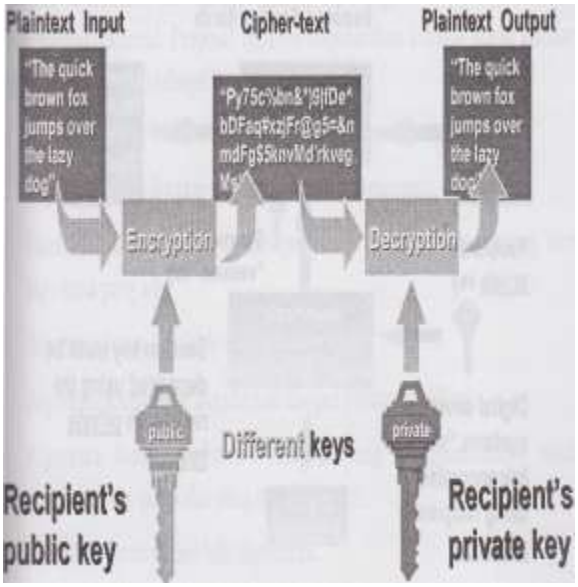
LANDASAN TEORI

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. Crypto berarti *secret* (rahasia) dan graphia berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain



Gambar 2. 1 Ilustrasi Algoritma Kriptografi Kunci Simetri

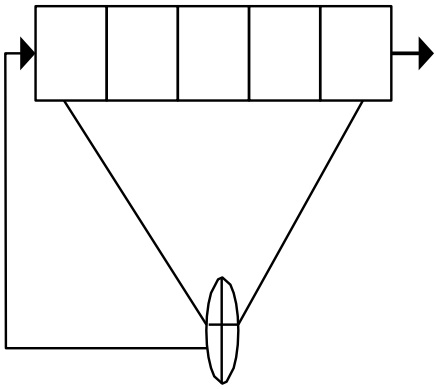
Ilustrasi dari algoritma kriptografi kunci asimetri dapat dilihat



Gambar 2. 2 Ilustrasi Algoritma Kriptografi Kunci Asimetri

P-ISSN : 2580-4316
E-ISSN : 2654-8054 https://doi.org/10.37817/ikraith-informatika.v11i2

Pada setiap saat isi sel dari register digeser (*shift*) ke kanan sejauh satu posisi, dan hasil operasi XOR terhadap subset dari isi sel ditempatkan pada sel paling kiri. Satu bit dari *output* biasanya diturunkan selama prosedur *update* ini.

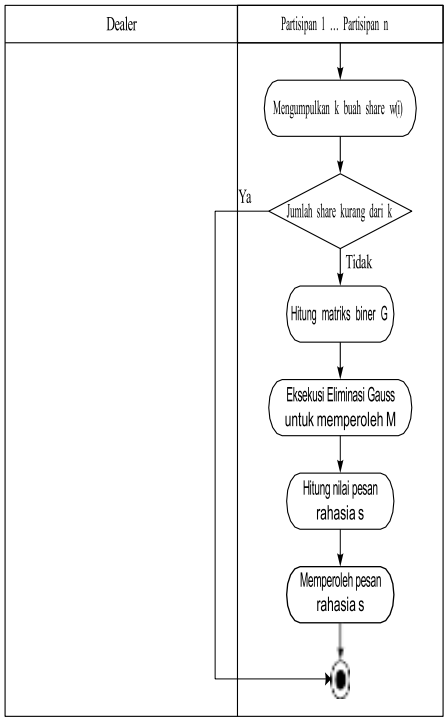


Gambar 2. 3 Linear Feedback Shift Register (LFSR)

METODOLOGI PENELITIAN

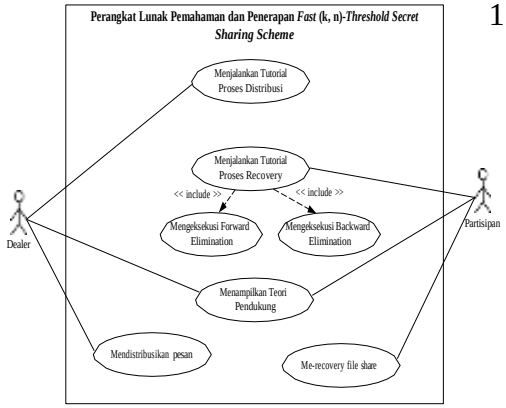
Untuk bagian, nilai k dan n dengan nilai maksimal 10, sedangkan untuk bagian aplikasi, nilai k dan n dibatasi maksimal 50, dimana $k \leq n$.

1. Untuk bagian pemahaman, pesan rahasia dengan panjang maksimal 50 karakter, sedangkan untuk bagian aplikasi, panjang pesan rahasia maksimal 1000 karakter.
2. rahasia berekstensi akan menghasilkan beberapa *file share* yang berekstensi *.kdi.
3. Pembangkitan dan pengujian bilangan prima menggunakan metode Rabin-Miller.



Gambar 3. 1 *Activity Diagram* dari Prosedur Kerja

P-ISSN : 2580-4316
E-ISSN : 2654-8054
https://doi.org/10.37817/ikraith-informatika.v11i2



3.1 Diagram

Rancangan tampilan dari *form* Main ini dapat dilihat pada gambar 3.3 berikut:



Gambar 3. 2 Rancangan *Form* Main

1. Perangkat lunak dapat digunakan untuk memahami prosedur kerja dari metode *Fast* (k, n) -*Threshold Secret Sharing Scheme*, yaitu melalui fasilitas 'Pemahaman' yang disediakan oleh perangkat lunak.
2. Perangkat lunak juga dapat digunakan untuk melakukan pengamanan data *file* teks, yaitu melalui fasilitas 'Aplikasi' yang disediakan oleh perangkat lunak
3. Perangkat lunak dapat dikembangkan dengan merancang suatu *class* dari metode *Fast* (k, n)-*Threshold Secret Sharing Scheme* sehingga metode ini dapat diterapkan pada aplikasi lainnya.

Perangkat lunak dapat dikembangkan dengan menerapkan metode ini untuk melakukan pengamanan *file* selain *text file* seperti *file audio*, *video*, gambar dan sebagainya.

P-ISSN : 2580-4316
E-ISSN : 2654-8054 https://doi.org/10.37817/ikraith-informatika.v11i2

DAFTAR PUSTAKA

Penerbit Andi, 2018.

Kendall, K.E. dan Kendall, J.E., Analisis dan Perancangan Sistem, Jilid 1, Alih Bahasa Thamir Abdul Hafedh Al-Hamdany, Prenhallindo, Jakarta.

Kurihara, , Kiyomoto, S., Fukushima, K., Tanaka, T., Jepang.

Code in C, *Second Edition*, John Willey and Sons Inc.

Stallings, W., *Cryptography and Network Security : Principle and Practice*, *Second Edition*, Prentice Hall.