

**PERANCANGAN *WEBSITE* LAYANAN PENGAMANAN
DATA RAHASIA DENGAN METODE ENKRIPSI
RABIN DAN *SHAMIR SECRET SHARING***

SKRIPSI

Oleh:

STEVEN ALVIN ALAMSYAH

NIM.1944074



**JENJANG PENDIDIKAN STRATA-1
PROGRAM STUDI TEKNIK INFORMATIKA
STMIK TIME
MEDAN
2024**

LEMBAR PENGESAHAN

**PERANCANGAN *WEBSITE* LAYANAN PENGAMANAN
DATA RAHASIA DENGAN METODE ENKRIPSI
RABIN DAN *SHAMIR SECRET SHARING***

SKRIPSI

Diajukan Untuk Melengkapi Persyaratan Guna
Mendapat Gelar Sarjana Strata Satu
Program Studi Teknik Informatika

Oleh:

STEVEN ALVIN ALAMSYAH

NIM.1944074

Disetujui Oleh:

Dosen Pembimbing I



Robet, M.Kom

Dosen Pembimbing II



Hendri, M.Kom

Medan, 06 Agustus 2024
Diketahui dan Disahkan Oleh:

Ketua STMIK TIME

Ketua Program Studi



Dr. Edi Wijaya, S.Kom., M.Kom., M.M

Robet, M.Kom

Kepada
Yth Ketua STMIK TIME
Dr. Edi Wijaya, S.Kom., M.Kom., M.M
di Medan

Hal : **Surat Pernyataan Bebas Plagiat**

Saya yang bertanda tangan di bawah ini :

Nama	: Steven Alvin Alamsyah
NIM	: 1944074
Program Studi	: Teknik Informatika
Angkatan	: 2019
Judul Skripsi	: Perancangan <i>Website</i> Layanan Pengamanan Data Rahasia Dengan Metode Enkripsi <i>Rabin</i> dan <i>Shamir Secret Sharing</i>

Dengan ini menyatakan bahwa skripsi yang Saya tulis adalah karya ilmiah asli dari pikiran saya sendiri.

Apabila kemudian hari terbukti bahwa skripsi tersebut merupakan Plagiat, maka saya bersedia gelar dan ijazah yang saya peroleh ditinjau kembali.

Demikian surat pernyataan ini Saya perbuat dengan pikiran yang sehat, tanpa tekanan dari siapapun.

Diketahui oleh
Pembantu Ketua I



Hendri, M.Kom

Medan, 06 Agustus 2024

Yang membuat pernyataan



Steven Alvin Alamsyah

ABSTRAK

Keamanan data rahasia di era digital menjadi salah satu perhatian utama, terutama dengan meningkatnya risiko kejahatan siber yang dapat mengancam informasi yang disimpan secara daring. Penelitian ini bertujuan untuk merancang sebuah website yang menggunakan kombinasi metode enkripsi *Rabin* dan *Shamir Secret Sharing* untuk meningkatkan keamanan data rahasia. Metode enkripsi *Rabin* digunakan untuk mengubah pesan asli menjadi ciphertext yang tidak dapat dibaca tanpa proses dekripsi, sementara metode *Shamir Secret Sharing* membagi ciphertext tersebut menjadi beberapa bagian (*shares*) yang hanya dapat digabungkan kembali oleh sejumlah *shares* yang cukup untuk merekonstruksi data asli. Implementasi ini memungkinkan pengamanan data yang lebih kuat, memastikan bahwa data rahasia tetap terlindungi meskipun sebagian dari media penyimpanan mengalami kerusakan atau hilang. Website yang dibangun dapat menjadi alat bantu yang efektif bagi masyarakat dalam mengamankan pesan rahasia serta memberikan kontribusi akademik sebagai referensi dalam mempelajari kriptografi.

Kata Kunci: Enkripsi *Rabin*, *Shamir Secret Sharing*, Keamanan Data

ABSTRACT

The security of confidential data in the digital era has become a major concern, especially with the increasing risk of cybercrime that can threaten information stored online. This research aims to design a website that utilizes a combination of Rabin encryption and Shamir Secret Sharing methods to enhance the security of confidential data. The Rabin encryption method is used to transform the original message into ciphertext that cannot be read without the proper decryption process, while the Shamir Secret Sharing method divides the ciphertext into several parts (shares) that can only be reassembled by a sufficient number of shares to reconstruct the original data. This implementation allows for stronger data protection, ensuring that confidential data remains secure even if some of the storage media is damaged or lost. The developed website can serve as an effective tool for the public in securing confidential messages and contribute academically as a reference for studying cryptography.

Keywords: *Rabin Encryption, Shamir Secret Sharing, Data Security*

KATA PENGANTAR

Ucapan puji dan syukur kepada hadirat Tuhan Yang Maha Esa atas segala berkat, hikmat, dan pertolongan-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi ini tepat pada waktunya.

Skripsi yang berjudul “**Perancangan Website Layanan Pengamanan Data Rahasia dengan metode enkripsi Rabin dan Shamir Secret Sharing**” ini disusun untuk memenuhi salah satu syarat dalam menyelesaikan pendidikan Program Strata I pada Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Time Program Studi Teknik Informatika. Penulis berharap agar hasil dari penelitian yang dilakukan ini dapat membawa banyak manfaat bagi berbagai pihak.

Dalam menyelesaikan tugas akhir ini, penulis banyak mendapat bantuan dari berbagai pihak. Oleh karena itu, melalui kesempatan ini penulis ingin menyampaikan terima kasih kepada:

1. Bapak Robet, M.Kom., selaku Dosen Pembimbing I dan Ketua Program Studi Teknik Informatika STMIK TIME Medan yang telah membimbing penulis selama mengerjakan skripsi ini.
2. Bapak Hendri, M.Kom, selaku Dosen Pembimbing II dan Pembantu Ketua I STMIK TIME Medan yang telah membimbing penulis selama mengerjakan skripsi ini.
3. Bapak Simon Kangga Lee, selaku Ketua Yayasan STMIK TIME Medan.
4. Bapak Dr. Edi Wijaya, S.Kom., M.Kom., M.M, selaku Ketua STMIK TIME Medan.
5. Seluruh Dosen STMIK TIME Medan yang telah mendidik dan membimbing penulis selama masa perkuliahan.
6. Teristimewa kepada orang tua dan keluarga tercinta, yang telah memberikan dukungan baik moral maupun materi kepada penulis selama ini.
7. Seluruh teman yang telah banyak membantu penulis dan memberikan dorongan serta semangat dalam menyelesaikan skripsi ini

8. Semua yang telah membantu penulis dalam menyelesaikan skripsi ini yang tidak dapat disebutkan satu persatu

Penulis menyadari dalam proses penyelesaian skripsi ini masih jauh dari sempurna, mengingat keterbatasan kemampuan yang penulis miliki dan terbatasnya waktu yang digunakan. Untuk itu, penulis mengharapkan saran, kritikan, dan masukan yang membangun demi perkembangan dan kemajuan penelitian selanjutnya. Semoga penulisan skripsi ini dapat bermanfaat bagi pihak yang berkepentingan.

Akhir kata penulis berharap agar laporan penulisan Tugas Akhir ini dapat berguna dan bermanfaat bagi pembaca.

Medan, 06 Agustus 2024

Penulis,

Steven Alvin Alamsyah

NIM. 1944074

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR.....	iii
DAFTAR ISI.....	v
DAFTAR GAMBAR.....	vii
DAFTAR TABEL	viii
DAFTAR LAMPIRAN	ix
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan dan Manfaat Penelitian	4
1.5 Metodologi Penelitian.....	4
1.6 Analisis Sistem.....	6
1.7 Perancangan Sistem	7
1.8 Sistematika Penulisan	7
BAB II TINJAUAN PUSTAKA.....	9
2.1 Konsep Sistem Informasi	9
2.1.1 Sistem.....	9
2.1.2 Informasi	12
2.1.3 Sistem Informasi	14
2.2 Website.....	16
2.3 Keamanan Data.....	19
2.4 Kriptografi.....	21
2.5 Metode <i>Rabin</i>	24
2.6 Metode <i>Shamir Secret Sharing</i>	25
2.7 <i>Use Case Diagram</i>	26
2.8 <i>Entity Relationship Diagram</i>	28

BAB III METODE PENELITIAN.....	29
3.1 Analisis Masalah.....	29
3.1.1 Analisis Proses Yang Berjalan Sesuai di Lapangan.....	29
3.1.2 Analisis Metode Yang Digunakan	30
3.1.3 Analisis Sistem Usulan	32
3.2 Perancangan	35
3.2.1 Perancangan Tampilan	35
3.2.2 Perancangan Basis Data	42
BAB IV HASIL DAN PEMBAHASAN	44
4.1 Hasil	44
4.2 Pembahasan.....	48
BAB V KESIMPULAN DAN SARAN	50
5.1 Kesimpulan	50
5.2 Saran	50
DAFTAR PUSTAKA	52
LAMPIRAN	

DAFTAR GAMBAR

Gambar 3.1 <i>Use Case Diagram</i> Sistem Usulan	33
Gambar 3.2 Rancangan Tampilan Awal	36
Gambar 3.3 Rancangan Tampilan Mengamankan Data Rahasia	37
Gambar 3.4 Rancangan Tampilan Berhasil Melakukan Pengamanan Data Rahasia	38
Gambar 3.5 Rancangan Tampilan Membuka Data Rahasia	39
Gambar 3.6 Rancangan Tampilan Berhasil Membuka Data Rahasia	40
Gambar 3.7 Rancangan Tampilan Gagal Membuka Data Rahasia	41
Gambar 3.8 Rancangan Basis Data Sistem Usulan	42
Gambar 4.1 Tampilan Awal	44
Gambar 4.2 Tampilan Mengamankan Data Rahasia	45
Gambar 4.3 Tampilan Berhasil Melakukan Pengamanan Data Rahasia	45
Gambar 4.4 Hasil Enkripsi Data Rahasia	46
Gambar 4.5 Tampilan Membuka Data Rahasia	46
Gambar 4.6 Tampilan Berhasil Membuka Data Rahasia	47
Gambar 4.7 <i>File</i> Hasil Dekripsi	47
Gambar 4.8 Tampilan Gagal Membuka Data Rahasia	48

DAFTAR TABEL

Tabel 1.1 Jadwal Penelitian.....	5
Tabel 2.1 Simbol <i>Use Case Diagram</i> [23].....	27
Tabel 2.2 Simbol <i>Entity Relationship Diagram</i> [23]	28
Tabel 3.1 Skenario <i>Use Case</i> Mengamankan Data Rahasia	33
Tabel 3.2 Skenario <i>Use Case</i> Membuka Data Rahasia.....	34
Tabel 3.3 Struktur Tabel Users	42
Tabel 3.4 Struktur Tabel Data_rahasia.....	42

DAFTAR LAMPIRAN

Lampiran 1 Daftar Riwayat Hidup

Lampiran 2 Surat Keputusan Dosen Pembimbing Skripsi

Lampiran 3 Kartu Bimbingan Dosen I

Lampiran 4 Kartu Bimbingan Dosen II

Lampiran 5 *Listing* Program

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era digital saat ini, keamanan dari data yang bersifat rahasia adalah hal penting yang harus dipertimbangkan [1]. Seiring dengan semakin berkembangnya teknologi informasi dan komunikasi serta dengan adanya penemuan *internet* telah mengakibatkan terjadinya perubahan drastis dalam berbagai aktivitas kehidupan manusia sehingga sangat diperlukan pelindungan informasi dalam *platform* digital untuk menghindari tindakan kejahatan siber [2]. Penyimpanan data pada *cloud computing* (seperti *Google Drive* atau *Dropbox*) mempunyai beberapa kekurangan seperti dapat terjadi pencurian data, rentan terhadap serangan siber, tidak dapat mengontrol keberadaan data, dapat terjadi pemutusan layanan, dan harus disediakan sistem operasi yang cocok dengan aplikasi [3]. Sedangkan, penyimpanan data pada berbagai media penyimpanan (seperti *harddisk*, *flashdisk*, CD) juga rentan terhadap terjadinya kerusakan ataupun kehilangan media penyimpanan tersebut [4].

Masalah keamanan data dapat diselesaikan dengan menggunakan metode kriptografi [5]. Kriptografi merupakan seni dan ilmu untuk menjaga keamanan data. Dalam menjaga keamanan data, kriptografi mengubah data pesan asli (*plaintext*) ke bentuk pesan terenkripsi (*ciphertext*) yang tidak terdefinisi isinya [6]. Metode enkripsi yang dipilih adalah metode enkripsi *Rabin*. Penelitian mengenai metode enkripsi *Rabin* yang pernah dilakukan sebelumnya seperti

Implementasi Algoritma Kriptografi *Rabin* dan *Lempel-Ziv-Welch* (LZW) dalam Pengamanan dan Kompresi File Citra, dimana algoritma Rabin merupakan salah satu sistem kriptografi asimetris yang kemampuan keamanannya terbukti karena menggunakan metode pemfaktoran bilangan yang sampai saat ini belum terpecahkan [7].

Untuk meningkatkan keamanan dari data rahasia, maka pada penelitian ini akan dikombinasikan metode enkripsi dengan metode *secret sharing*. *Secret sharing scheme* merupakan metode untuk melakukan pembagian suatu *secret*, biasanya berupa kunci, menjadi beberapa bagian yang disebut *share* [8]. Kriptografi *secret sharing* menggunakan skema (m,n) -*threshold*, yaitu data rahasia akan dipecahkan menjadi beberapa bagian sehingga sembarang m dari n orang ($m \leq n$) yang memiliki pecahan data rahasia dapat menggabungkan atau memperoleh kembali isi data rahasia tersebut [9]. Untuk metode *secret sharing* dipilih metode *Shamir secret sharing*. Penelitian mengenai metode *secret sharing Shamir* yang pernah dilakukan sebelumnya seperti Implementasi *Secure Multi-Party Computation Menggunakan Metode Shamir Secret Sharing* pada Pengamanan Dokumen Digital Rahasia, dimana metode *Sharing secret sharing* ini dipilih karena tingkat keamanan dari algoritma *Shamir Secret Sharing Scheme* juga terbukti aman [1]. Penelitian lainnya yaitu Implementasi Algoritme *Trivium Stream Cipher* dan *Shamir's Secret Sharing* pada *File Portable Document Format* (PDF), dimana algoritma *Shamir's Secret Sharing* dapat memberikan aspek *availability*, hal ini dapat dibuktikan dengan pengujian *share* dan *reconstruct* yang dapat dikatakan valid pada saat pengujian [10].

Berdasarkan uraian di atas, maka penulis tertarik untuk menerapkan kombinasi metode enkripsi *Rabin* dan *Shamir Secret Sharing* dalam pengamanan data rahasia secara *online* dengan mengambil skripsi yang berjudul **“Perancangan Website Layanan Pengamanan Data Rahasia dengan Metode Enkripsi *Rabin* dan *Shamir Secret Sharing*”**.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan sebelumnya, maka rumusan masalah pada penelitian ini yaitu:

1. Bagaimana menerapkan metode enkripsi *Rabin* untuk mengamankan pesan rahasia?
2. Bagaimana menerapkan metode *Shamir Secret Sharing* dalam memecahkan *ciphertext* menjadi beberapa bagian?

1.3 Batasan Masalah

Berikut ini akan diuraikan batasan masalah pada penelitian ini agar penelitian dapat diselesaikan pada waktunya antara lain:

1. Panjang pesan rahasia yang dimasukkan minimal 1 karakter dan maksimal 10.000 karakter.
2. *File* yang dapat diproses hanya *file* dokumen *Microsoft Word* dengan format *.docx.
3. *File* hasil pecahan rahasia yang dihasilkan memiliki format *.enc.
4. Nilai kunci yang diperlukan dalam metode *Rabin* dibatasi antara 2 digit sampai 6 digital bilangan bulat positif, dengan pertimbangan nilai kunci

yang terlalu besar akan menyebabkan proses eksekusi metode memerlukan waktu yang lama.

5. Jumlah pecahan rahasia dibatasi minimal 2 dan maksimal 100, dengan pertimbangan bahwa jumlah pecahan rahasia yang banyak akan menyebabkan proses penggabungan pada metode *Shamir Secret Sharing* menjadi lama.

1.4 Tujuan dan Manfaat Penelitian

Tujuan yang diharapkan dalam penelitian ini adalah:

1. Untuk menerapkan metode enkripsi *Rabin* untuk mengamankan pesan rahasia.
2. Untuk menerapkan metode *Shamir Secret Sharing* dalam memecahkan *ciphertext* menjadi beberapa bagian.

Manfaat yang diharapkan dalam penelitian ini adalah:

1. *Website* dapat digunakan untuk membantu masyarakat dalam mengamankan pesan rahasia.
2. Laporan tugas akhir dapat dijadikan sebagai referensi dalam mempelajari mengenai metode kriptografi.

1.5 Metodologi Penelitian

Metodologi penelitian yang akan digunakan dalam penelitian ini diuraikan sebagai berikut:

1. Jadwal Penelitian

Berikut ini akan diuraikan tabel jadwal penelitian dari awal penelitian hingga penelitian selesai yang dapat dilihat pada Tabel 1.1.

Tabel 1.1 Jadwal Penelitian

NO	Waktu Ket.	2023								2024															
		November				Desember				Januari				Februari				Maret				April			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Rumusan Masalah																								
2	Pengumpulan Data																								
3	Analisis Sistem																								
4	Perancangan Sistem																								
5	Uji Coba Sistem																								
6	Penulisan Laporan																								

2. Bahan dan Alat

Berikut ini akan dijelaskan bahan dan alat yang digunakan yaitu berupa *hardware* dan *software* yang digunakan dalam proses penelitian.

Hardware yang digunakan yaitu sebuah laptop dengan spesifikasi:

- Processor Intel Core i5.
- RAM 8 GB.
- Harddisk 2 TB.

Software yang digunakan yaitu:

- Sistem Operasi Windows 10 64 Bit.
- Bahasa pemrograman python versi 3.7 (64-bit).

3. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan pada penelitian ini antara lain sebagai berikut:

a. Metode Kooperatif

Melakukan pengumpulan data dengan menjawab keadaan sebab akibat serta penyebab utama yang dihadapi dari pengamanan data di masyarakat.

b. Metode Studi Pustaka

Mengumpulkan data-data teori melalui jurnal, media cetak, ataupun sumber-sumber referensi dari internet.

1.6 Analisis Sistem

Analisis sistem pada penelitian ini terbagi menjadi 3 tahapan proses yaitu:

1. Analisis proses berjalan sesuai di lapangan yaitu melakukan analisis sistem berjalan yang digunakan saat ini khususnya sistem berjalan yang digunakan dalam pengamanan data rahasia.
2. Analisis metode yang digunakan yaitu dengan mendeskripsikan contoh perhitungan metode enkripsi *Rabin* dan *Shamir Secret Sharing*.
3. Analisis sistem usulan yaitu menggambarkan sistem usulan yang akan dibangun beserta fitur-fitur yang tersedia yang dimodelkan dengan menggunakan *tools* pemodelan sistem *Use Case Diagram*.

1.7 Perancangan Sistem

Perancangan sistem pada penelitian ini dilakukan dengan melakukan perancangan *prototype* tampilan dengan menggunakan *software* Balsamiq Mockup 3.

1.8 Sistematika Penulisan

Untuk mempermudah memahami permasalahan yang dibahas, maka skripsi ini akan disusun dengan sistematika sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini diuraikan tentang latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metodologi penelitian serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini akan dibahas mengenai landasan dan kajian teori-teori yang berhubungan dengan judul penulisan skripsi serta penelitian terdahulu yang sudah dilakukan sebelumnya.

BAB III METODE PENELITIAN

Pada bab ini membahas tentang tahapan-tahapan metode penelitian yang dilakukan dengan poin utama yaitu pada analisis dan perancangan. Analisis ini akan menguraikan tentang analisis sistem berjalan, analisis metode yang digunakan serta analisis sistem usulan.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini akan diuraikan tahapan yang penulis lakukan dalam mengembangkan sistem, desain, hasil *testing* dan implementasinya. Dari hasil yang didapat akan dilakukan pembahasan yang berisikan tentang hasil penelitian yang didapatkan.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisikan mengenai kesimpulan yang didapatkan setelah melakukan penelitian dengan proses analisa terhadap teori dan hasil pengujian. Dan juga terdapat saran yang berisikan hal-hal yang belum berhasil dan masih mengalami masalah berdasarkan hasil pengujian yang dilakukan.

BAB II

TINJAUAN PUSTAKA

2.1 Konsep Sistem Informasi

Secara umum, konsep dari sistem informasi disusun oleh 2 bagian yaitu sistem dan informasi.

2.1.1 Sistem

Sistem adalah suatu kumpulan dari prosedur-prosedur, saling berhubungan dan membentuk jaringan kerja untuk mencapai tujuan tertentu. Secara sederhana sistem dapat diartikan sebagai suatu kumpulan atau himpunan dari unsur, komponen, atau variabel yang terorganisir, saling berinteraksi, saling tergantung satu sama lain, dan terpadu [11].

Sistem merupakan kumpulan dari beberapa bagian yang memiliki keterkaitan dan saling bekerja sama serta membentuk suatu kesatuan untuk mencapai tujuan dari sistem tersebut [12].

Sistem adalah sekumpulan unsur/elemen yang saling berkaitan dan saling mempengaruhi dalam melakukan kegiatan bersama untuk mencapai suatu tujuan [13].

Suatu sistem untuk mencapai tujuan tertentu harus memiliki sifat-sifat dasar yang menjadikannya suatu karakter. Suatu sistem untuk mencapai tujuan tertentu harus memiliki sifat-sifat dasar yang menjadikannya suatu karakter. Karakteristik suatu sistem terdiri dari komponen-komponen (*components*), batas

sistem (*boundary*), lingkungan luar sistem (*environments*), penghubung (*interface*), masukan (*input*), keluaran (*output*), pengolah (*process*), dan sasaran (*objectives*) atau tujuan (*goal*) [11].

1. Komponen Sistem

Suatu sistem terdiri dari sejumlah komponen yang saling berinteraksi membentuk satu kesatuan. Komponen-komponen sistem dapat berupa suatu sub sistem. Setiap sub sistem mempunyai sifat-sifat dari sistem yang menjalankan suatu fungsi tertentu dan mempengaruhi proses sistem secara keseluruhan.

2. Batas Sistem

Batas sistem merupakan daerah yang membatasi antara suatu sistem dengan sistem lainnya atau lingkungan luarnya. Batas sistem ini memungkinkan suatu sistem dipandang sebagai suatu kesatuan.

3. Lingkungan Luar Sistem

Lingkungan luar dari suatu sistem adalah apapun diluar batas dari sistem yang mempengaruhi operasi sistem, dapat bersifat menguntungkan maupun merugikan. Lingkungan luar yang menguntungkan merupakan energi dari sistem yang harus dijaga dan dipelihara. Sedangkan lingkungan luar yang merugikan harus ditahan dan dikendalikan, karena akan mengganggu kelangsungan hidup dari sistem.

4. Penghubung Sistem

Penghubung merupakan media penghubung antara satu sub sistem dengan sub sistem lainnya. Keluaran (*output*) dari satu sub sistem akan menjadi

masukan (*input*) untuk sub sistem yang lainnya dengan melalui penghubung.

5. Masukan Sistem

Masukan sistem adalah energi yang dimasukkan ke dalam sistem. Masukan dapat berupa masukan perawatan (*maintenance input*) dan masukan sinyal (*signal input*). *Maintenance input* adalah energi yang dimasukkan supaya sistem tersebut dapat beroperasi. *Signal input* adalah energi yang diproses untuk didapatkan keluaran.

6. Keluaran Sistem

Keluaran sistem adalah hasil dari energi yang diolah dan diklasifikan menjadi keluaran yang berguna dan sisi pembuangan. Keluaran dapat merupakan masukan untuk sub sistem yang lain atau kepada super sistem.

7. Pengolah Sistem

Suatu sistem dapat mempunyai suatu bagian pengolah atau sistem itu sendiri sebagai pengolahnya. Pengolah yang akan mengubah masukan menjadi keluaran.

8. Sasaran sistem

Suatu sistem pasti mempunyai sasaran (*objectives*) atau tujuan (*goal*), kalau tidak mempunyai sasaran maka operasi sistem tidak akan ada gunanya. Suatu sistem dikatakan berhasil bila mengenai sasaran atau tujuannya.

Berdasarkan informasi dari berbagai sumber tersebut, dapat disimpulkan bahwa sistem adalah suatu entitas terorganisir yang terdiri dari berbagai komponen atau unsur yang saling berinteraksi dan bekerja sama untuk mencapai

tujuan tertentu. Sistem memiliki karakteristik dasar yang mencakup komponen sistem, batas sistem, lingkungan luar sistem, penghubung sistem, masukan sistem, keluaran sistem, pengolah sistem, dan sasaran sistem.

2.1.2 Informasi

Informasi merupakan hasil pengolahan data sehingga menjadi bentuk yang penting bagi penerimanya dan mempunyai kegunaan sebagai dasar dalam pengambilan keputusan yang dapat dirasakan akibatnya secara langsung saat itu juga atau secara tidak langsung pada saat mendatang [14].

Informasi adalah data yang telah diproses, diorganisasikan atau diringkas menjadi sesuatu yang berguna [12].

Informasi adalah aset yang sangat vital dalam sebuah organisasi dan wajib diproteksi karena informasi merupakan aset yang berharga bagi organisasi [15].

Informasi harus memiliki nilai jika dapat mengubah tindakan yang diambil. Perubahan ini penting untuk dipahami karena data sebenarnya tidak memiliki nilai dalam pengambilan keputusan, hanya informasi yang memiliki nilai, dalam arti informasi memudahkan manajer dalam mengambil keputusan. Informasi adalah data yang diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi penerimanya. Sumber informasi adalah data. Data nyata akan menggambarkan suatu kejadian-kejadian dan kesatuan nyata [14].

Data yang diolah untuk menghasilkan informasi menggunakan model proses yang tertentu. Data yang diolah melalui suatu model menjadi informasi, kemudian penerima menerima informasi tersebut, yang berarti menghasilkan suatu keputusan dan melakukan tindakan yang lain akan membuat sejumlah data

kembali. Data tersebut akan di *input*, diproses kembali lewat suatu model yang disebut dengan siklus informasi (*information cycle*). Siklus ini juga disebut dengan siklus pengelolaan data (*data processing cycles*). Kualitas informasi terdiri dari 3 hal yaitu [11]:

1. Informasi harus akurat (*accurate*) berarti informasi harus bebas dari kesalahan-kesalahan dan tidak menyesatkan.
2. Tepat pada waktunya (*time lines*) merupakan informasi yang datang pada penerima tidak boleh terlambat. Informasi yang sudah asing tidak akan memiliki nilai lagi.
3. Relevan (*relevance*) berarti informasi tersebut mempunyai manfaat untuk pemakaiannya. Relevansi informasi untuk tiap-tiap orang satu dengan yang lainnya berbeda.

Berdasarkan informasi dari berbagai sumber tersebut, dapat disimpulkan bahwa informasi adalah hasil pengolahan data yang telah diproses, diorganisir, atau diringkas sehingga menjadi sesuatu yang memiliki nilai dan kegunaan bagi penerimanya. Informasi memiliki peran penting sebagai dasar dalam pengambilan keputusan, baik secara langsung pada saat itu juga maupun secara tidak langsung pada masa mendatang.

Lebih lanjut, informasi dianggap sebagai aset vital dalam sebuah organisasi dan perlu diproteksi karena nilainya yang berharga. Proses transformasi data menjadi informasi melibatkan suatu model proses, yang sering disebut sebagai siklus informasi atau siklus pengelolaan data. Data yang diolah melalui siklus ini menjadi informasi, yang kemudian diterima oleh penerima,

menghasilkan keputusan, dan memicu tindakan yang dapat menghasilkan sejumlah data kembali.

Kualitas informasi juga menjadi hal krusial, dengan tiga elemen utama, yaitu keakuratan (*accurate*), ketepatan waktu (*time lines*), dan relevansi (*relevance*). Informasi harus bebas dari kesalahan dan tidak menyesatkan (akurat), harus disampaikan pada waktu yang tepat tanpa terlambat (tepat pada waktunya), dan harus memiliki manfaat atau relevansi bagi pemakainya.

Dengan demikian, informasi bukan hanya sekadar data yang diolah, tetapi merupakan output yang bernilai tinggi, mampu membantu pengambilan keputusan, dan memiliki dampak yang signifikan pada tindakan organisasi. Oleh karena itu, perlindungan dan manajemen kualitas informasi menjadi suatu keharusan dalam lingkungan organisasi modern.

2.1.3 Sistem Informasi

Sistem informasi merupakan sekumpulan *hardware*, *software*, *brainware*, prosedur, dan atau aturan yang diorganisasikan secara integral untuk mengolah data menjadi informasi yang bermanfaat guna untuk memecahkan masalah dan pengambilan keputusan. Sistem informasi adalah kesatuan data olahan yang terintegrasi dan saling melengkapi yang menghasilkan *output* baik dalam bentuk gambar, suara maupun tulisan [11].

Sistem informasi adalah sebuah sistem yang terdiri dari entitas-entitas yang saling berhubungan dan bekerjasama untuk mengumpulkan, mengolah, menyimpan, mengelola, dan mendistribusikan informasi guna mendukung

pengambilan keputusan, pengawasa, analisis, dan pengelolaan suatu organisasi atau bisnis [15].

Sistem informasi adalah suatu sistem yang menyediakan informasi untuk mengambil keputusan dan juga menjalankan suatu bisnis yang ada di perusahaan [16].

Sistem informasi juga dapat dikatakan sebagai kombinasi antara prosedur kerja, informasi, orang, dan teknologi informasi yang diorganisasikan untuk mencapai tujuan dalam sebuah organisasi. Pendapat tersebut mengemukakan, bahwa sistem informasi merupakan kumpulan kegiatan yang diintegrasikan antara program kerja, informasi ke dalam suatu *server database* sehingga keinginan suatu organisasi dalam mencapai tujuan bisa terwujud [11].

Komponen sistem informasi terdiri dari [11]:

1. *Hardware* (perangkat keras), terdiri dari komputer, printer dan jaringan.
2. *Software*, kumpulan perintah yang ditulis dengan aturan untuk memerintah komputer melaksanakan tugas tertentu.
3. Data, merupakan komponen dasar dari informasi yang akan diproses lebih lanjut untuk menghasilkan informasi
4. Manusia, yang terlibat dalam komponen seperti operator dan pimpinan.
5. Prosedur, dokumentasi proses sistem buku penuntun operasional (aplikasi) dan teknis.

Sistem Informasi memiliki tujuan di antaranya adalah suatu sistem informasi yang baik haruslah relevan agar dapat memperoleh hasil yang bagus dalam menentukan suatu keputusan dalam sebuah kelompok. Seluruh komponen

sistem informasi dan data-data, harus memberikan hasil yang bermanfaat sekurang-kurangnya sebanyak pengeluaran yang telah dilakukan [17].

Peranan sistem informasi yang sering kita jumpai dalam kehidupan sehari-hari, contoh di antaranya yaitu [17]:

1. Sistem akademis berbasis *website*, yang dapat mempermudah kita untuk mengakses data terkait akademisi.
2. Sistem pemerintahan berbasis *website*, atau *e-goverment*, yang dapat memberikan layanan pemerintahan melalui internet.
3. Sistem pertukaran data digital, dengan menggunakan komputer kita dapat bertukar data secara cepat.
4. Sistem biometrik yaitu sistem yang dikembangkan untuk keamanan informasi dengan menggunakan pola wajah dan sidik jari agar tidak sembarang orang melakukan akses.

Berdasarkan informasi dari berbagai sumber tersebut, dapat disimpulkan bahwa sistem informasi adalah suatu kumpulan komponen yang terintegrasi, termasuk *hardware*, *software*, *brainware*, prosedur, dan aturan, yang bekerja bersama untuk mengolah data menjadi informasi yang bermanfaat. Sistem informasi tidak hanya mencakup teknologi, tetapi juga melibatkan manusia dan prosedur dalam rangka mencapai tujuan suatu organisasi atau bisnis.

2.2 Website

Website merupakan kumpulan halaman digital yang berisi informasi berupa teks, animasi, gambar, suara dan video atau gabungan dari semuanya yang

terkoneksi oleh internet, sehingga dapat dilihat oleh seluruh siapapun yang terkoneksi jaringan internet. Jenis kategori *website* antara lain [18]:

1. *Web statis* Merupakan *website* yang mempunyai halaman yang tidak berubah. Perubahan suatu halaman dilakukan secara manual dengan meng-*edit code* yang menjadi stuktur dari *website* tersebut.
2. *Web dinamis* Merupakan *website* yang secara terstruktur diperuntukan untuk di-*update* sesering mungkin. Biasanya disediakan halaman backend untuk melakukan perubahan konten dari *website* tersebut. Contohnya : *web portal*, *web berita*, dll.
3. *Web interaktif* merupakan *website* yang berinteraksi antara penggunanya. Biasanya berupa forum diskusi maupun *blog*. Dimana adanya moderator sebagai pengatur alur diskusi.

Pemrograman *web* adalah pembuatan aplikasi program dengan bahasa skrip yang akan menghasilkan sebuah aplikasi yang diakses pada *web browser*. Ada beberapa istilah yang sering digunakan apabila anda mempelajari pemrograman *web* ini diantaranya yaitu [18]:

1. *Internet*.
Internet berarti rangkaian komputer yang terhubung menjadi beberapa rangkaian jaringan. Sistem komputer terhubung secara global dan menggunakan TCP/IP sebagai protocol. Melalui internet pertukaran informasi dapat dilakukan tanpa batas asalkan kedua pihak terhubung kedalam jaringan yang sama.
2. *World Wide Web (WWW)*.

WWW merupakan kumpulan *web server* diseluruh dunia yang dapat menyediakan data dan informasi untuk dapat digunakan secara massal.

3. *Website.*

Website merupakan istilah yang merujuk kepada suatu nama halaman *web* yang dapat diakses jika terkoneksi dengan internet. Untuk mengakses sebuah *website*, selain terkoneksi dengan internet, anda pun harus membukanya dalam sebuah aplikasi web browser.

4. *Web Server.*

Web server merupakan perangkat lunak yang digunakan untuk menerima permintaan melalui protokol HTTP atau HTTPS dari *client*, kemudian dikirimkan kembali dalam bentuk halaman-halaman *web*. Contoh *web server*: Xampp, Apache2Triad, dll. +

5. URL (*Universal Resource Locator*).

URL merupakan suatu alamat yang menunjukkan sebuah halaman tertentu internet. Contoh URL adalah: <http://www.google.com>.

6. HTTP (*Hypertext Transfer Protocol*).

HTTP merupakan bagian dari URL digunakan untuk mengidentifikasi lokasi *web*, dan digunakan dalam protokol HTML.

7. DNS (*Domain Name System*).

DNS merupakan sistem database terdistribusi yang tidak banyak dipengaruhi oleh bertambahnya *database*. DNS menjamin informasi *host* terbaru akan disebarkan ke jaringan bila diperlukan.

8. IP (*Internet Protocol*).

IP (*Internet Protocol*) merupakan protokol yang digunakan dalam internet, secara teknis bermakna suatu bentuk pengisian dan pengalamatan data-data dan informasi yang akan dikirim melalui internet.

9. *Hyperlink.*

Hyperlink atau disebut *link* merupakan sebuah tools yang berperan dalam mempopulerkan penggunaan internet, *hyperlink* dapat mereferensikan sebuah teks atau gambar ke alamat lain di internet.

10. *Web browser.*

Menggunakan *web browser* mudah, yang diperlukan hanyalah harus memiliki alamat *web* yang akan dibuka. Alamat ini biasa disebut dengan *Uniform Resource Locator* (URL). Jika menggunakan sistem operasi Windows terdapat program *web browser* bawaan, yaitu *Internet Explorer*. Terdapat banyak program alternative *web browser* yang sebagian besar bersifat gratis, seperti *Firefox*, *Opera*, *Safari*, *Chrome* dan seterusnya.

2.3 Keamanan Data

Keamanan data adalah serangkaian prinsip, teknik, dan konsep yang digunakan untuk melindungi data dari akses yang tidak sah, penggunaan yang tidak sah, modifikasi, atau pengungkapan yang tidak sah. Beberapa konsep inti dalam keamanan data meliputi [19]:

1. *Kerahasiaan (Confidentiality).*

Melibatkan kebijakan dan teknologi untuk mencegah akses yang tidak sah terhadap data. Ini dapat dicapai melalui enkripsi data, manajemen hak akses, dan penggunaan teknik otentikasi yang kuat.

2. Integritas (*Integrity*).

Memastikan bahwa data tidak dimodifikasi secara tidak sah selama penyimpanan, pemindahan, atau pengolahan. Teknik seperti penandaan waktu, hash functions, dan pengecekan tanda tangan digital digunakan untuk memverifikasi integritas data.

3. Ketersediaan (*Availability*).

Menjamin bahwa data tersedia dan dapat diakses oleh pengguna yang berwenang ketika dibutuhkan. Ini melibatkan praktik-praktik redundansi, backup, dan pemulihan bencana untuk menghindari kehilangan data atau gangguan layanan.

4. Otentikasi (*Authentication*).

Verifikasi identitas pengguna atau sistem sebelum memberikan akses ke data. Metode otentikasi dapat mencakup penggunaan password, kunci kriptografis, atau metode biometrik.

5. Otorisasi (*Authorization*).

Membatasi akses ke data berdasarkan hak-hak pengguna yang telah ditetapkan. Ini melibatkan pemberian izin dan hak akses yang sesuai kepada pengguna atau entitas yang sah.

6. Non-repudiasi (*Non-repudiation*).

Mencegah pengguna untuk menyangkal tindakan yang telah mereka lakukan atau pesan yang telah mereka kirimkan. Ini sering dicapai melalui penggunaan tanda tangan digital atau sistem audit yang kuat.

7. Privasi (*Privacy*).

Menjaga keamanan dan kerahasiaan data pribadi dan sensitif. Perlindungan privasi dapat dicapai melalui enkripsi data, anonimisasi, dan kebijakan privasi yang ketat.

8. Keamanan Fisik (*Physical Security*).

Melindungi infrastruktur fisik yang menyimpan atau mengakses data dari akses yang tidak sah atau kejadian yang merusak.

2.4 Kriptografi

Salah satu metode pengamanan yang dapat dilakukan untuk pengamanan pesan adalah dengan menggunakan kriptografi. Kriptografi telah digunakan selama berabad-abad oleh raja dan ratu di Eropa untuk memberi perintah terhadap pasukan perang mereka. Hal ini dilakukan untuk menghindari informasi penting tersebut jatuh ke tangan orang yang salah sehingga dapat membongkar rahasia kerajaan. Ancaman dari para musuh tersebut yang memotivasi untuk melakukan pengkodean dan enkripsi terhadap pesan sehingga dengan kunci yang tepat hanya orang tertentu saja yang dapat membaca pesan tersebut [20].

Kriptografi adalah ilmu yang menggunakan teknik matematika yang berhubungan dengan aspek keamanan informasi. Kriptografi adalah ilmu yang mempelajari bagaimana membuat pesan yang dikirim dapat sampai kepada penerima dengan aman. Pesan asli yang dimengerti isinya/maknanya dinamakan plainteks. Pesan yang tidak dimengerti, yang merupakan hasil transformasi dari plainteks disebut cipherteks. Sementara itu, kriptografi memiliki tiga karakteristik utama yaitu operasi yang digunakan untuk mengubah plainteks ke cipherteks, kunci yang digunakan, dan bagaimana plainteks tersebut di proses [20].

Kriptografi (*Chryptography*) berasal dari bahasa Yunani yaitu *Kryptos* yang artinya tersembunyi dan *graphien* yang artinya tulisan. Secara harfiah, kriptografi dapat diartikan sebagai tulisan yang tersembunyi atau tulisan yang dirahasiakan. Kriptografi merupakan suatu cara menjaga agar pesan tetap aman dari pihak ketiga. Kriptografi adalah ilmu yang mempelajari dalam merahasiakan pesan. Pesan asli disebut dengan plainteks sedangkan pesan yang telah di sandikan disebut dengan cipherteks. Proses dalam merubah plainteks ke cipherteks disebut dengan enkripsi. Proses merubah cipherteks ke plainteks disebut dengan dekripsi [20].

Beberapa istilah yang berhubungan dengan transformasi dari plainteks ke cipherteks diantaranya adalah *cipher*, kunci, *encipher*, *decipher*, kriptanalisis, dan kriptologi. *Cipher* adalah algoritma yang digunakan untuk melakukan transformasi plainteks ke cipherteks. Kunci adalah beberapa informasi kritis yang diperlukan *cipher*, dimana kunci ini hanya diketahui oleh pengirim dan penerima pesan. *Encipher* adalah proses mentransformasi plainteks ke cipherteks dengan menggunakan cipher dan kunci. *Decipher* adalah proses transformasi cipherteks kembali ke plainteks dengan menggunakan cipher dan kunci. Kriptanalisis (*cyptanalysis*) adalah ilmu yang mempelajari prinsip-prinsip atau metode-metode mentransformasikan cipherteks kembali ke plainteks tanpa mengetahui kunci untuk decipher. Sedangkan kriptologi (*cryptology*) adalah ilmu yang berhubungan dengan kriptografi dan kriptanalisis [20].

Teknik yang digunakan untuk mendekripsi pesan tanpa mengetahui pengetahuan mengenai detail pengenkripsian disebut dengan kriptanalisis

(*Cryptanalysis*). Kriptografi dan kriptanalisis selanjutnya disebut dengan kriptologi. Sistem kriptografi terdiri dari 5 bagian yakni [20]:

1. Plainteks (M).

Plainteks adalah pesan atau data masukan yang bentuk aslinya dapat dimengerti maknanya. Plainteks merupakan masukan untuk enkripsi.

2. Kunci rahasia (K).

Kunci rahasia juga merupakan masukan untuk enkripsi. Kunci rahasia adalah nilai bebas yang nantinya akan dikenakan terhadap teks asli dan mempengaruhi keluaran.

3. Cipherteks (C).

Cipherteks adalah hasil dari algoritma enkripsi yang tidak dapat diketahui lagi makna sebenarnya.

4. Algoritma enkripsi (EK).

Algoritma enkripsi (E_k) Memiliki dua data masukan yakni plaintexts dan kunci rahasia. Algoritma enkripsi melakukan transformasi dari plaintexts sehingga menghasilkan pesan yang telah disandikan. $E_k: M \rightarrow C$, dimana $k \in K$

5. Algoritma dekripsi (DK).

Memiliki dua data masukan yakni pesan yang sudah disandikan (cipherteks) dan kunci rahasia. Merupakan algoritma mengembalikan cipherteks menjadi plaintexts. $D_k: C \rightarrow M$, mana $k \in K$.

Dalam perkembangannya, kriptografi memiliki dua jenis algoritma, yaitu: algoritma enkripsi kunci simetri (*symmetrickey encryption algorithm*) dan algoritma enkripsi kunci publik/asimetri (*public-key encryption algorithm*).

Algoritma enkripsi kunci simetri menggunakan kunci yang sama atau disebut juga kunci rahasia, baik untuk enkripsi maupun dekripsi. Oleh karena itu kunci ini harus dirahasiakan oleh pengirim dan penerima pesan agar cipherteks tetap aman dari gangguan serangan. Algoritma enkripsi kunci publik menggunakan dua kunci pasangan namun berbeda. Satu kunci dipakai untuk enkripsi, yaitu kunci publik, pasangan kuncinya digunakan untuk dekripsi, yaitu kunci privat [20].

2.5 Metode *Rabin*

Metode Rabin merupakan salah satu metode kriptografi kunci-publik. Metode ini menggunakan satu pasang kunci yaitu kunci publik dan kunci privat. Kunci publik digunakan dalam proses enkripsi sedangkan kunci privat digunakan dalam proses dekripsi. Pada proses dekripsi, algoritma rabin menghasilkan 4 buah *plaintext*. Oleh karena itu, diperlukan modifikasi dalam proses dekripsi untuk menentukan plaintext yang sebenarnya. Berikut ini cara kerja dari metode *Rabin* antara lain [21]:

1. Pembangkitan Kunci Rabin.

Berikut ini adalah algoritma proses pembangkitan kunci pada algoritma *Rabin Public Key*:

- a. Pilih dua bilangan prima besar sembarang, p dan q , dimana keduanya kongruen terhadap $3 \bmod 4$. Atau dengan kata lain, jika p dan q dimodulokan 4 akan menghasilkan 3 dapat dilihat pada persamaan 2.1.

$$p \equiv q \equiv 3 \pmod{4} \quad (2.1)$$

- b. n merupakan kunci publik yang diperoleh dengan rumus seperti yang ditunjukkan pada persamaan 2.2.

$$n = p \cdot q \quad (2.2)$$

- c. Simpan dan rahasiakan nilai p dan q (*private key*), sedangkan nilai n (*public key*) dapat disebarluaskan seluas-luasnya.

2. Enkripsi Rabin.

Proses enkripsi pada algoritma *Rabin Public Key* menggunakan kunci publik n . Untuk melakukan enkripsi pesan (m), m harus lebih kecil dari n . Berikut adalah rumus untuk melakukan enkripsi pada algoritma *Rabin Public Key* dapat dilihat pada persamaan 2.3.

$$c = m^2 \bmod n \quad (2.3)$$

Dimana:

$c = \text{ciphertext}$

$m = \text{plaintext/message}$

$n = \text{kunci public}$

2.6 Metode Shamir Secret Sharing

Shamir Secret Sharing memanfaatkan ide dari persoalan interpolasi. Dari persoalan ini didapatkan untuk membentuk polynomial [22].

$$y = a_0 + a_1x + \dots + a_nx_n \quad (2.4)$$

diperlukan $n + 1$ titik. Nilai a_0 sampai a_n dapat diperoleh dengan membuat $n + 1$ buah persamaan linier (linear). Persamaan-persamaan linier ini lalu diselesaikan. Salah satu cara menyelesaikan persamaan-persamaan linier ini adalah dengan metode Gauss [22].

Shamir Secret Sharing juga menggunakan skema ambang (*threshold schemes*). Skema ambang adalah metode pembagian *secret* S kepada n partisipan

sedemikian sehingga sembarang himpunan bagian yang terdiri dari t partisipan dapat merekonstruksi S , tetapi jika kurang dari t maka S tidak dapat direkonstruksi [22].

Algoritma pembagian *share* pada skema ambang adalah [22]:

1. Pilih bilangan prima p , yang harus lebih besar dari semua kemungkinan nilai secret S dan juga lebih besar dari jumlah n partisipan. Semua komputasi dilakukan dalam modulus p .
2. Pilih $t - 1$ buah bilangan bulat acak dalam modulus p , misalkan $a_1, a_2, \dots, a_{t-1}$ dan nyatakan polinomial:

$$f(x) = S + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \pmod{p} \quad (2.5)$$

sedemikian sehingga $f(0) \equiv S \pmod{p}$.

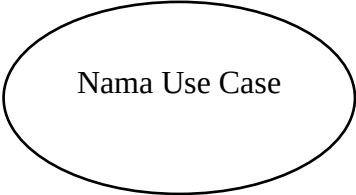
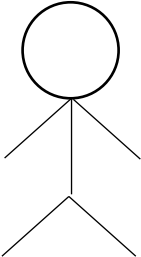
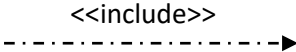
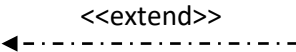
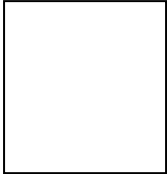
3. Untuk n partisipan, kita pilih integer berbeda, $x_1, x_2, \dots, x_n \pmod{p}$ dan setiap orang memperoleh share (x_i, y_i) yang dalam hal ini.

$$y = f(x_i) \pmod{p} \quad (2.6)$$

2.7 Use Case Diagram

Use Case Diagram adalah salah satu alat pemodelan sistem yang merupakan komponen dari *Unified Modeling Language* (UML) yang digunakan untuk menggambarkan interaksi antara pengguna dan sistem. Penggunaan *Diagram Use Case* dapat memberikan gambaran yang efektif dalam menjelaskan konteks suatu sistem dengan jelas, sehingga memperlihatkan batasan sistem tersebut dengan jelas. Terdapat beberapa simbol-simbol dari *Use Case Diagram* seperti yang ditunjukkan pada Tabel 2.1 berikut [23].

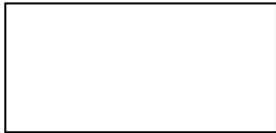
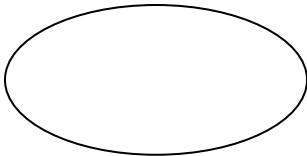
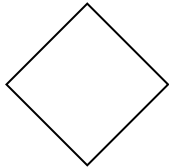
Tabel 2.1 Simbol *Use Case Diagram* [23]

Nama	Simbol	Deskripsi
<i>Use Case</i>		Simbol yang menggambarkan fungsi dari sistem umumnya diekspresikan dalam bentuk kata kerja di awal setiap frasa.
Aktor		Simbol yang mewakili pengguna yang terlibat dalam <i>Use Case</i> biasanya menyatakan orang-orang yang berinteraksi dengan sistem.
Asosiasi		Simbol yang menghubungkan antara <i>Use Case</i> dan aktor menggambarkan komunikasi antara keduanya. Asosiasi digunakan untuk menggambarkan hubungan statis antara elemen-elemen tersebut.
<i>Include</i>		Simbol ini menggambarkan bahwa <i>Use Case</i> secara keseluruhan merupakan bagian dari fungsionalitas <i>Use Case</i> lainnya.
<i>Extend</i>		Simbol yang serupa dengan " <i>include</i> ", namun menunjukkan bahwa sebuah <i>Use Case</i> tambahan dapat berdiri sendiri tanpa membutuhkan <i>Use Case</i> yang ditambahkan.
Sistem		Simbol yang membatasi bahwa setiap interaksi dengan simbol lain harus berada di dalamnya.

2.8 Entity Relationship Diagram

Entity Relationship Diagram merupakan teknik pendekatan *top-bottom* untuk desain *database*, yang dilakukan dengan proses berupa identifikasi informasi penting kemudian menggambarannya dalam sebuah model. *Entity Relationship Diagram* adalah model yang berguna membantu dalam memahami data dan bagaimana data tersebut digunakan dalam sebuah perusahaan. Terdapat beberapa simbol-simbol dari *Use Case Diagram* seperti yang ditunjukkan pada Tabel 2.2 berikut [23].

Tabel 2.2 Simbol Entity Relationship Diagram [23]

Nama	Simbol	Deskripsi
Entitas		Kumpulan dari objek yang dapat diidentifikasi secara unik biasanya merupakan nama dari tabel di dalam rancangan basis data.
Atribut		Gambaran karakteristik dari sebuah entitas yang biasanya dianggap sebagai nama kolom di dalam rancangan basis data.
Hubungan		Menyatakan jumlah himpunan relasi antar entitas.
Garis		Penghubung entitas, atribut dan hubungan.

BAB III

METODE PENELITIAN

3.1 Analisis Masalah

Pada sub bab ini, akan dilakukan analisis mendalam terhadap masalah yang ingin diselesaikan. Dengan memahami secara menyeluruh tentang sumber masalah, konsekuensi yang dihadapi, dan faktor-faktor yang memengaruhinya, dapat dirancang solusi yang tepat dan efektif. Analisis masalah menjadi langkah kritis dalam proses pemecahan masalah yang dilakukan, yang akan membantu dalam menentukan arah dan pendekatan yang sesuai untuk mencapai tujuan penelitian. Analisis masalah dibagi menjadi 3 yaitu analisis proses yang berjalan sesuai di lapangan, analisis metode yang digunakan, dan analisis sistem usulan.

3.1.1 Analisis Proses Yang Berjalan Sesuai di Lapangan

Analisis proses berjalan sesuai di lapangan yaitu melakukan analisis sistem berjalan yang digunakan saat ini khususnya sistem berjalan yang digunakan dalam pengamanan data rahasia. Berikut ini uraiannya:

1. Penggunaan *Cloud Computing*: Banyak organisasi dan individu saat ini menggunakan layanan penyimpanan cloud seperti *Google Drive* atau *Dropbox* untuk menyimpan data rahasia. Namun, kelemahan-kelemahan seperti rentan terhadap serangan siber dan risiko pencurian data perlu dipertimbangkan.

2. Penyimpanan Data pada Media Fisik: Selain menggunakan layanan *cloud*, beberapa organisasi juga menyimpan data rahasia pada media fisik seperti *harddisk*, *flashdisk*, atau CD. Namun, media penyimpanan tersebut rentan terhadap kerusakan atau kehilangan.

Dengan mempertimbangkan kelemahan dan kelebihan dari sistem berjalan yang digunakan yang digunakan saat ini, penulis tertarik untuk menggabungkan metode enkripsi *Rabin* dengan metode *Shamir Secret Sharing* dalam pengamanan data rahasia. Hal ini mencerminkan upaya untuk meningkatkan keamanan data rahasia dengan memanfaatkan kelebihan dari kedua metode tersebut.

3.1.2 Analisis Metode Yang Digunakan

Analisis metode yang digunakan yaitu dengan mendeskripsikan contoh perhitungan metode enkripsi *Rabin* dan *Shamir Secret Sharing* dalam melakukan pengamanan data rahasia. Berikut ini uraian cara kerjanya:

1. Misalkan memiliki sebuah pesan rahasia yang akan diamankan menggunakan metode enkripsi *Rabin* dan metode *Shamir Secret Sharing*. Pesan rahasia tersebut adalah "RAHASIA".
2. Enkripsi dengan Metode *Rabin*:
 - a. Pesan "RAHASIA" dalam bilangan ASCII: 82, 65, 72, 65, 83, 73, 65.
 - b. Kunci enkripsi Rabin yang digunakan: 123.
 - c. Proses enkripsi dilakukan dengan menghitung $c = m^2 \bmod n$, dimana m adalah nilai ASCII pesan rahasia n adalah modulus.
 - d. Hasil enkripsi untuk setiap karakter pesan:

$$c_1 = 82^2 \bmod 123 = 52$$

$$c_2 = 65^2 \bmod 123 = 16$$

$$c_3 = 72^2 \bmod 123 = 9$$

$$c_4 = 65^2 \bmod 123 = 16$$

$$c_5 = 83^2 \bmod 123 = 25$$

$$c_6 = 73^2 \bmod 123 = 91$$

$$c_7 = 65^2 \bmod 123 = 16$$

e. Hasil enkripsi dalam bentuk bilangan: 52, 16, 9, 16, 25, 91, 16.

3. *Secret Sharing* dengan Metode *Shamir*:

a. Memilih parameter:

Pilih sebuah bilangan prima yang besar p sebagai modulus. Dalam kasus ini, akan dipilih $p = 127$, karena 127 adalah bilangan prima.

Pilih juga sebuah bilangan bulat a yang lebih kecil dari p , yang akan digunakan sebagai basis perhitungan. Misalkan $a=2$.

b. Menentukan kunci rahasia:

Kunci enkripsi *Rabin* yang digunakan adalah $k = 123$.

c. Menghitung bagian-bagian "*share*":

Dimembagi kunci enkripsi menjadi beberapa bagian "*share*". Dalam contoh ini, akan dibagi menjadi 3 bagian.

Setiap bagian "*share*" direpresentasikan oleh sebuah koefisien polinomial yang dihasilkan secara acak.

Koefisien polinomial $f(x)$ akan memiliki bentuk $f(x)=k+a_1x+a_2x^2+...+a_{t-1}x^{t-1}$, di mana t adalah jumlah total bagian "*share*" (3 dalam contoh ini).

d. Menghitung koefisien polinomial:

Dipilih $t-1$ koefisien acak $a_1, a_2, \dots, a_{t-1}$ dari himpunan bilangan bulat positif yang lebih kecil dari modulus p .

Misalkan memilih koefisien acak sebagai berikut:

$$a_1=7, a_2=12.$$

Dengan demikian, polinomial $f(x)$ akan menjadi $f(x)=123+7x+12x^2$.

- e. Menghitung Bagian-Bagian "*Share*" dari Polinomial:

Kita menghitung nilai y (bagian "*share*") untuk setiap x (nomor identifikasi), yaitu $f(x) \bmod p$.

$$\text{Misalkan } x_1=1, x_2=2, x_3=3.$$

Dengan menggunakan polinomial $f(x)=123+7x+12x^2$ dan modulus $p=127$, dapat dihitung nilai y sebagai berikut:

$$y_1=f(1) \bmod 127 = (123+7*1+12*1^2) \bmod 127 = 142 \bmod 127 = 15.$$

$$y_2=f(2) \bmod 127 = (123+7*2+12*2^2) \bmod 127 = 179 \bmod 127 = 52.$$

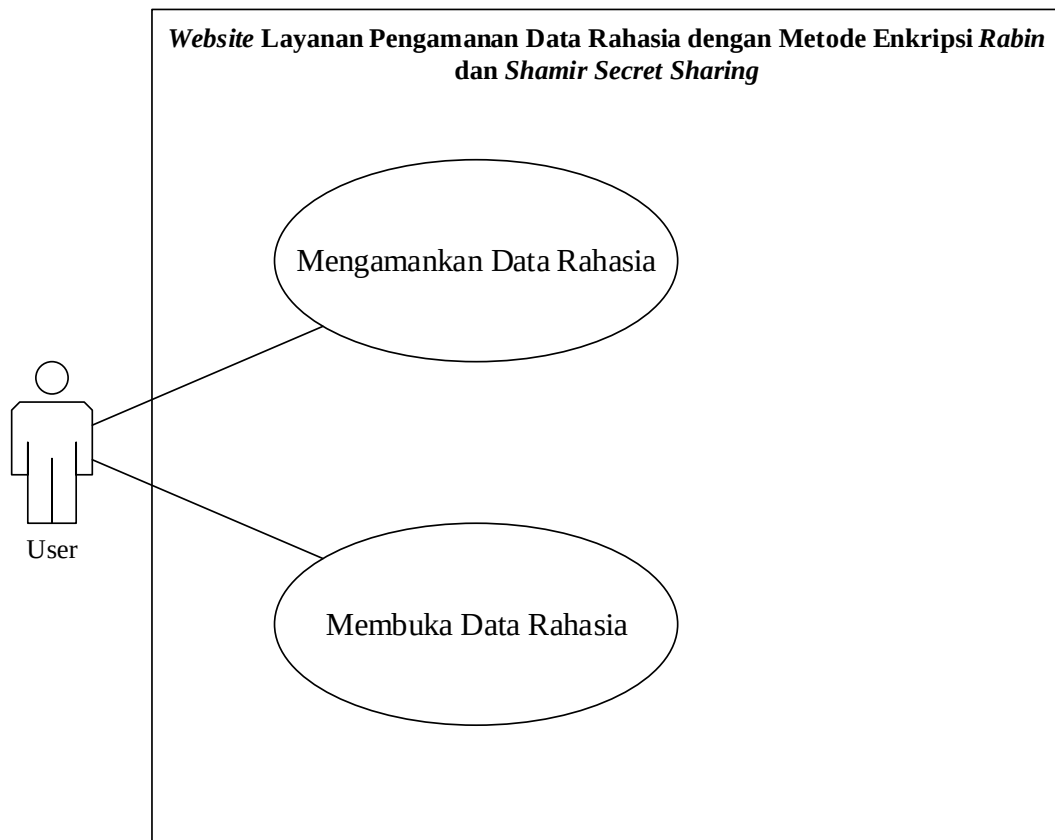
$$y_3=f(3) \bmod 127 = (123+7*3+12*3^2) \bmod 127 = 232 \bmod 127 = 105.$$

Dengan demikian, telah berhasil membagi kunci enkripsi *Rabin* 123 menjadi 3 bagian "*share*" menggunakan metode *Shamir Secret Sharing*. Bagian-bagian "*share*" ini adalah (1,15), (2,52), dan (3,105). Setiap bagian "*share*" ini harus disimpan secara aman, dan setidaknya 2 bagian diperlukan untuk mengembalikan kembali kunci enkripsi asli.

3.1.3 Analisis Sistem Usulan

Analisis sistem usulan yaitu menggambarkan sistem usulan yang akan dibangun beserta fitur-fitur yang tersedia yang dimodelkan dengan menggunakan

tools pemodelan sistem *Use Case Diagram*. Berikut ini, Gambar 3.1 menunjukkan *Use Case Diagram* dari sistem usulan.



Gambar 3.1 Use Case Diagram Sistem Usulan

Tahapan selanjutnya adalah membuat skenario dari setiap *Use Case* yang akan dibangun sehingga akan tampak secara jelas alur dan proses dari setiap aktor-aktor dalam menjalankan *Use Case* tersebut.

Tabel 3.1 dan Tabel 3.2 menunjukkan Skenario *Use Case*.

Tabel 3.1 Skenario Use Case Mengamankan Data Rahasia

Mengamankan Data Rahasia		Nama Use Case
<i>User</i>		Aktor
Melakukan pengamanan data rahasia dengan menggunakan metode <i>Rabin</i> dan <i>Shamir Secret Sharing</i>		Deskripsi
Aksi Aktor	Respon Sistem	

1. Masuk ke halaman <i>make secret</i>		Normal Flow Event
	2. Menampilkan halaman yang berisikan <i>form</i> pengamanan data rahasia	
3. Melakukan pengisian <i>form</i> dan melakukan <i>upload file word</i>		
4. Menekan tombol <i>submit</i>		
	5. Melakukan proses pengamanan data rahasia sesuai cara kerja metode <i>Rabin</i> dan <i>Shamir Secret Sharing</i>	
	6. Menampilkan kunci yang dibagi menjadi beberapa <i>fragment</i>	

Tabel 3.2 Skenario Use Case Membuka Data Rahasia

Membuka Data Rahasia		Nama Use Case
User		Aktor
Melakukan pembukaan data rahasia		Deskripsi
Aksi Aktor	Respon Sistem	
1. Masuk ke halaman <i>open secret</i>		Normal Flow Event
	2. Menampilkan halaman <i>form</i> pengisian <i>key fragment</i>	
3. Mengisi <i>key fragment</i> yang sesuai		
4. Menekan tombol <i>submit</i>		
	5. Menampilkan pesan berhasil membuka data rahasia dengan mengisi <i>pass code</i>	
6. Mengisikan <i>pass code</i> yang benar dan menekan tombol <i>download file now</i>		
	7. Mengunduh data	

	dokumen rahasia yang berhasil dibuka	
--	--------------------------------------	--

3.2 Perancangan

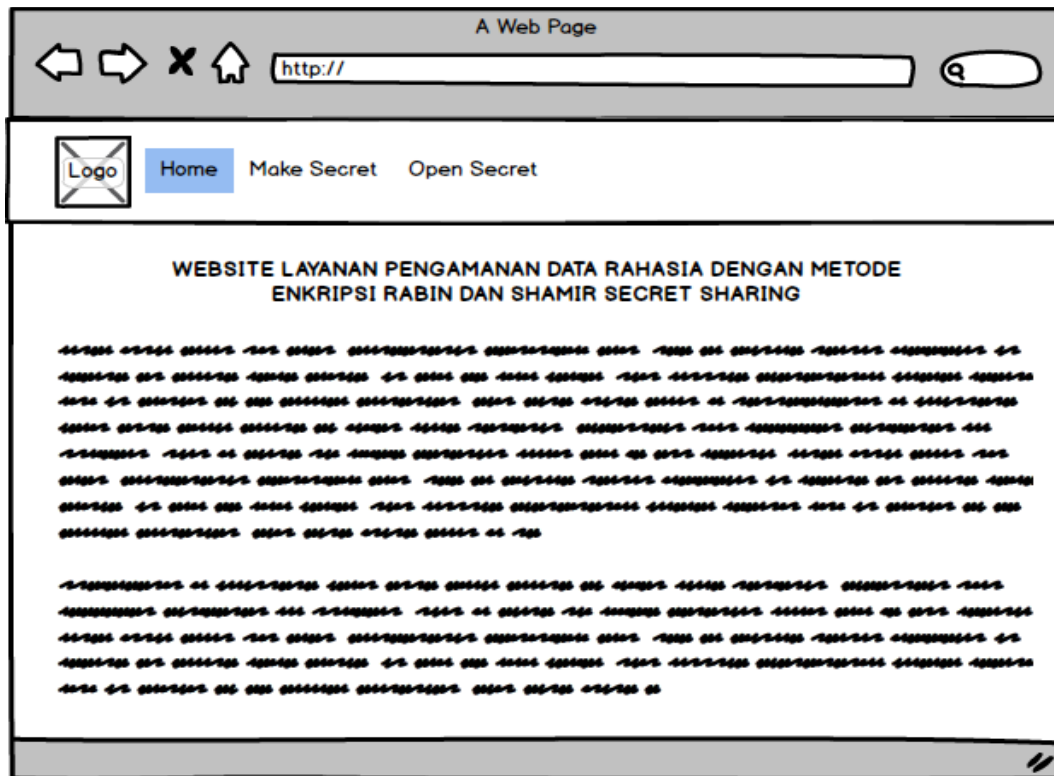
Perancangan pada penelitian ini dibagi menjadi 2 yaitu perancangan tampilan dan perancangan basis data.

3.2.1 Perancangan Tampilan

Perancangan tampilan diuraikan mengenai rancangan tampilan dari *website* layanan pengamanan data rahasia dengan metode enkripsi *Rabin* dan *Shamir Secret Sharing*. Berikut ini keseluruhan rancangan tampilan sistem tersebut antara lain:

1. Rancangan Tampilan Awal.

Tampilan awal berisikan pengenalan mengenai *website* yang dibangun.



Gambar 3.2 Rancangan Tampilan Awal

2. Rancangan Tampilan Mengamankan Data Rahasia.

Tampilan pengamanan data rahasia berisikan *form* untuk melakukan pengamanan data rahasia terhadap *file word*.

A Web Page

http://

Logo Home Make Secret Open Secret

Make Secret

Participants (Max. 100) *

xx

Pass Code *

Retype Pass-Code *

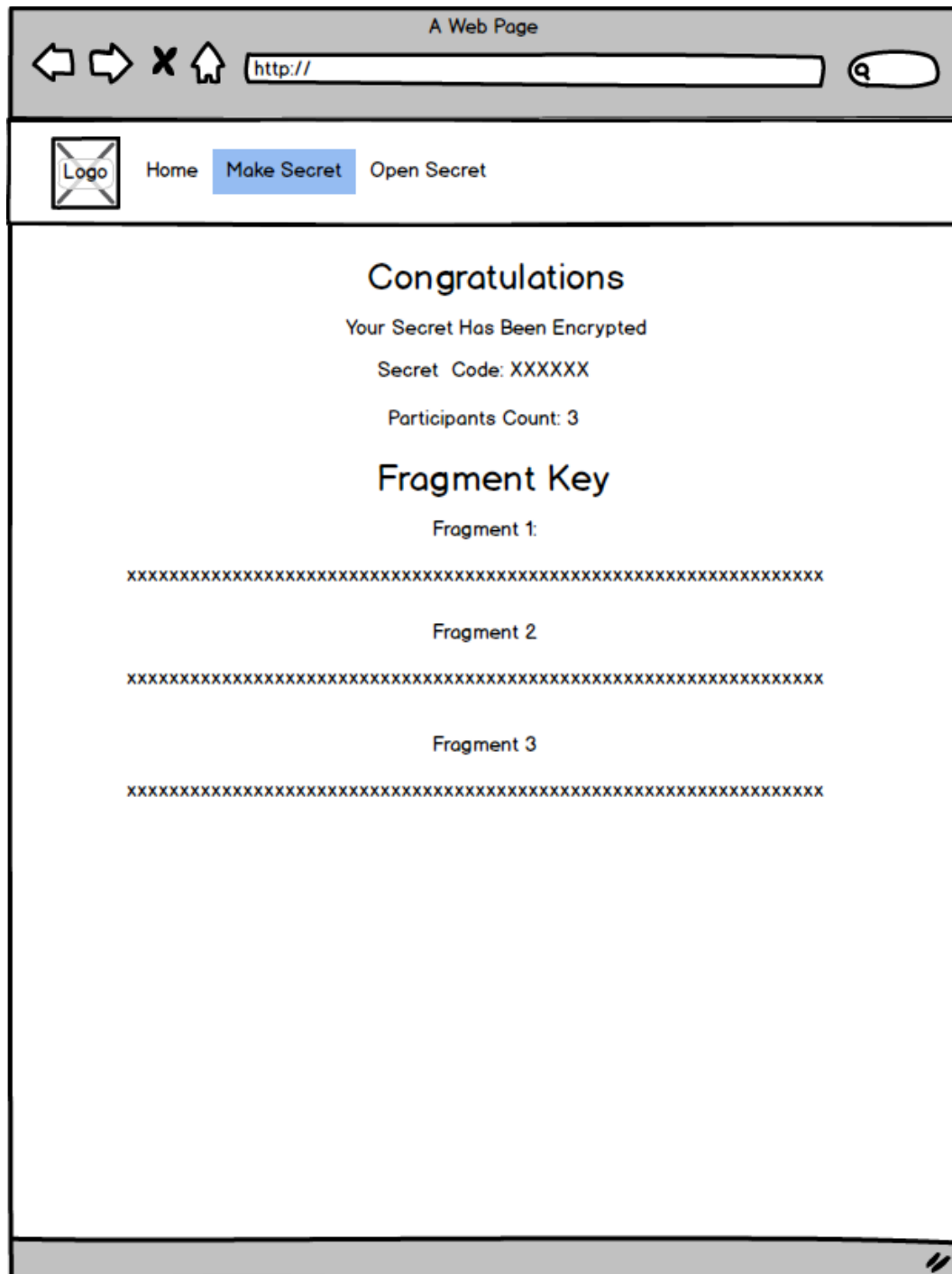
Select File to Upload *

Browse File No File Chosen

Submit

Gambar 3.3 Rancangan Tampilan Mengamankan Data Rahasia

3. Rancangan Tampilan Berhasil Melakukan Pengamanan Data Rahasia.
Tampilan ini berisikan pesan berhasil dan kunci-kunci yang terbentuk dari metode *Rabin Karp* dan *Shamir Secret Sharing*.



Gambar 3.4 Rancangan Tampilan Berhasil Melakukan Pengamanan Data

Rahasia

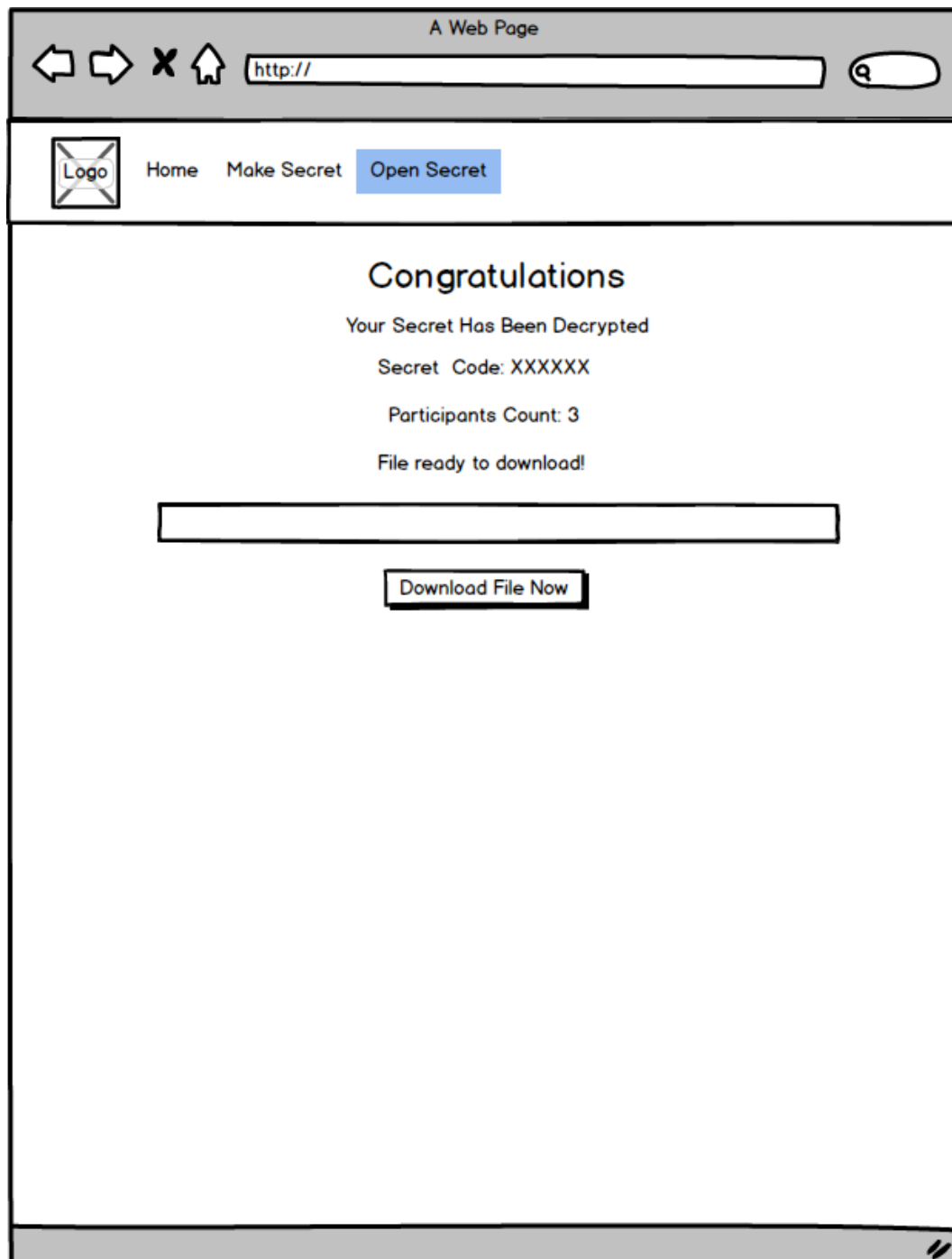
4. Rancangan Tampilan Membuka Data Rahasia.

Tampilan membuka data rahasia berisikan *form* untuk melakukan pembukaan data rahasia dengan memasukkan *secret code* terlebih dahulu barulah muncul jumlah *key fragment* yang perlu dimasukkan.

Gambar 3.5 Rancangan Tampilan Membuka Data Rahasia

5. Rancangan Tampilan Berhasil Membuka Data Rahasia.

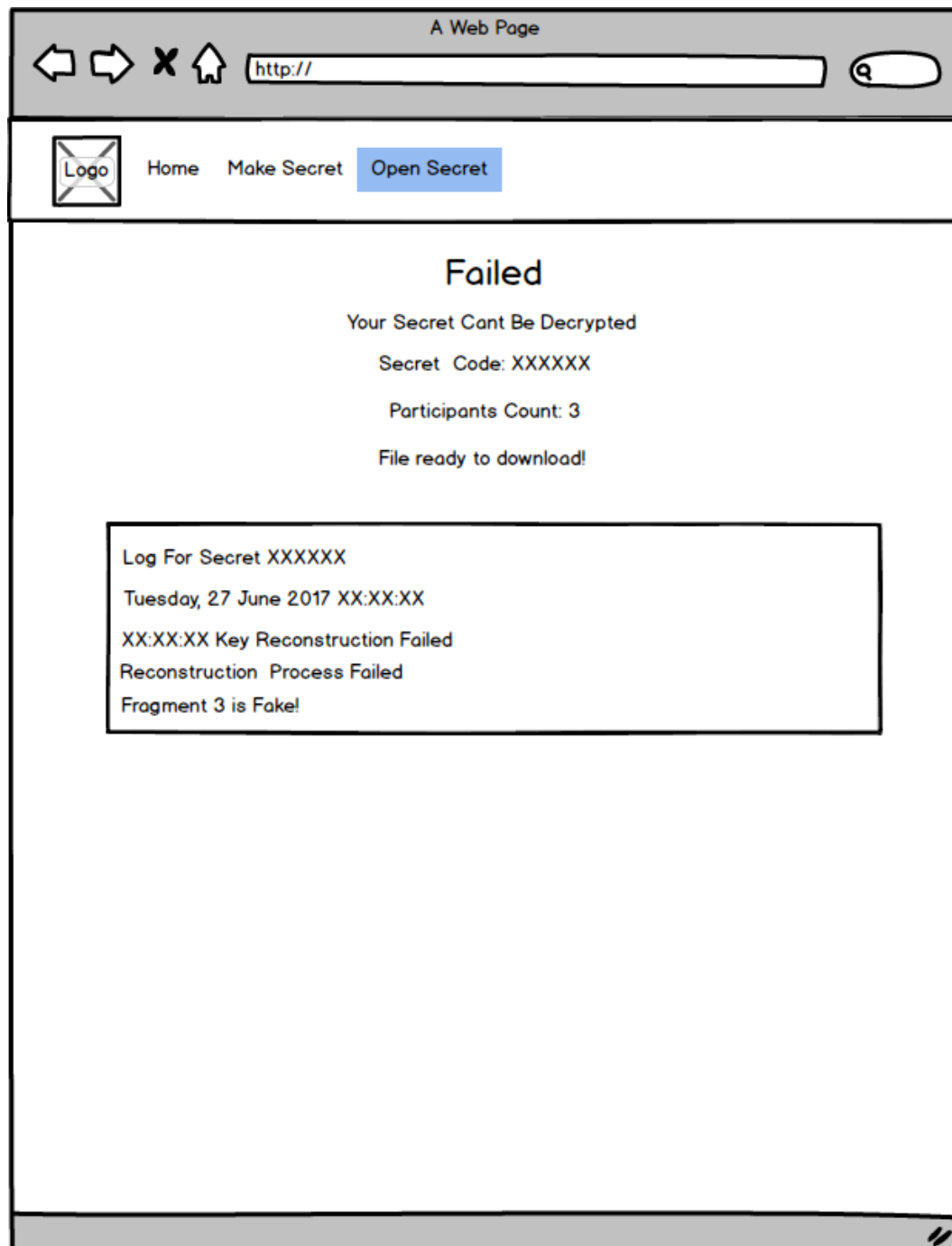
Tampilan berhasil membuka data rahasia berisikan pesan bahwa data rahasia berhasil dibuka dimana *user* harus memasukkan *pass code* untuk mengunduh dokumen *word* data rahasia.



Gambar 3.6 Rancangan Tampilan Berhasil Membuka Data Rahasia

6. Rancangan Tampilan Gagal Membuka Data Rahasia.

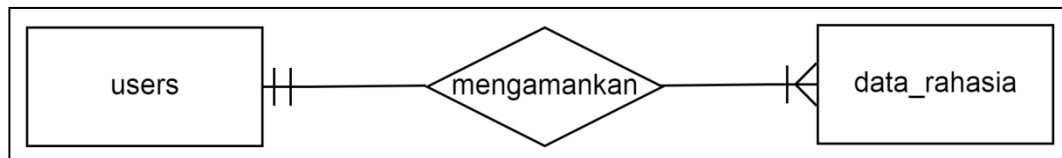
Tampilan gagal membuka data rahasia berisikan pesan proses pembukaan data rahasia gagal serta disertakan pesan alasan kegagalan dalam membuka data rahasia tersebut.



Gambar 3.7 Rancangan Tampilan Gagal Membuka Data Rahasia

3.2.2 Perancangan Basis Data

Perancangan basis data menggambarkan relasi dari tabel dalam basis data yang digunakan dalam menyusun *website* layanan pengamana data rahasia dengan metode *Rabin* dan *Shamir Secret Sharing*. Pemodelan rancangan basis data menggunakan *Entity Relationship Diagram* (ERD).



Gambar 3.8 Rancangan Basis Data Sistem Usulan

Tahap selanjutnya adalah menyusun struktur tabel dari setiap entitas-entitas yang ada.

Tabel 3.3 dan Tabel 3.4 menunjukkan Struktur Tabel.

Tabel 3.3 Struktur Tabel Users

Nama Field	Tipe Data	Null	Keterangan
ip_address	int(11)	No	ID <i>user</i> (primary key)
created_at	timestamp	No	Waktu pembuatan <i>user</i>
updated_at	timestamp	No	Waktu <i>update</i> data <i>user</i>

Tabel 3.4 Struktur Tabel Data_rahasia

Nama Field	Tipe Data	Null	Keterangan
secret_code	int(11)	No	Kode rahasia pengamanan data rahasia (primary key)
pass_code	varchar(60)	No	Kata sandi data rahasia
file_upload	text	No	Nama <i>file</i> yang di-

			<i>upload</i>
fragment_key	text	No	<i>Fragment</i> key
created_at	timestamp	No	Waktu melakukan pengamanan data rahasia
updated_at	timestamp	No	Waktu <i>update</i> melakukan pengamanan data rahasia

BAB IV

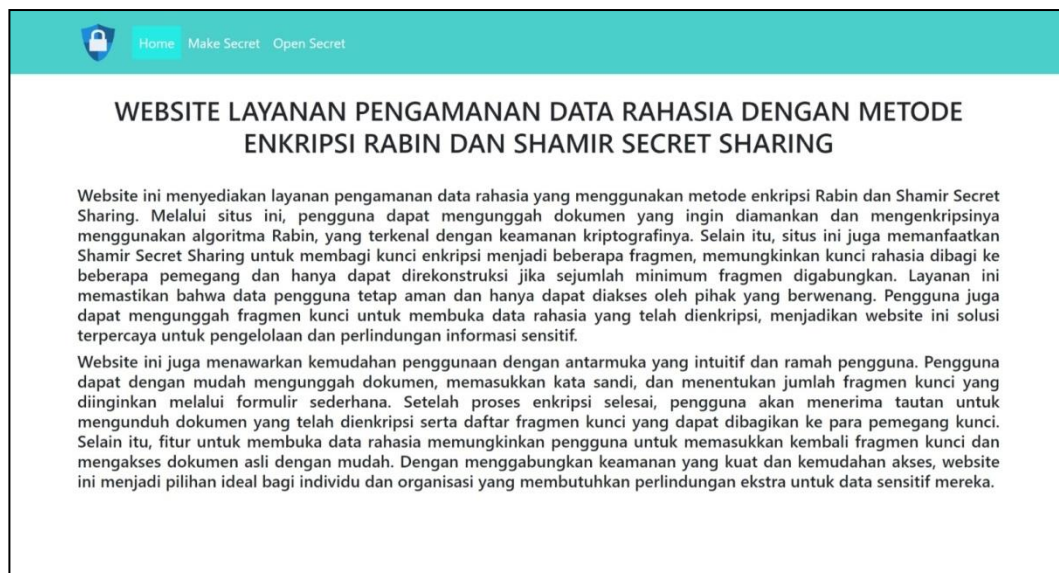
HASIL DAN PEMBAHASAN

4.1 Hasil

Hasil penelitian ini berupa dibangunnya sebuah *website* layanan pengamanan data rahasia dengan metode enkripsi *Rabin* dan *Shamir Secret Sharing*. Berikut ini keseluruhan rancangan tampilan sistem tersebut antara lain:

1. Tampilan Awal.

Tampilan awal berisikan pengenalan mengenai *website* yang dibangun.



Gambar 4.1 Tampilan Awal

2. Tampilan Mengamankan Data Rahasia.

Tampilan pengamanan data rahasia berisikan *form* untuk melakukan pengamanan data rahasia terhadap *file word*.

Gambar 4.2 Tampilan Mengamankan Data Rahasia

3. Tampilan Berhasil Melakukan Pengamanan Data Rahasia.

Tampilan ini berisikan pesan berhasil dan kunci-kunci yang terbentuk dari metode *Rabin Karp* dan *Shamir Secret Sharing*.

Gambar 4.3 Tampilan Berhasil Melakukan Pengamanan Data Rahasia

Data yang di-*upload* kemudian di enkripsi menjadi berekstensi *.enc* sehingga tidak dapat dibuka oleh siapapun. Untuk membuka data rahasia maka diperlukan proses dekripsi.

Name	Date modified	Type	Size
CW2-CIBM2024	7/31/2024 12:46 PM	Microsoft Word Doc...	79 KB
CW2-CIBM2024.docx.enc	7/31/2024 12:40 PM	ENC File	79 KB
Lagi_Data	7/31/2024 12:37 PM	Microsoft Word Doc...	13 KB
Lagi_Data.docx.enc	7/31/2024 12:36 PM	ENC File	13 KB
Test.docx.enc	7/31/2024 12:38 PM	ENC File	14 KB

Gambar 4.4 Hasil Enkripsi Data Rahasia

4. Tampilan Membuka Data Rahasia.

Tampilan membuka data rahasia berisikan *form* untuk melakukan pembukaan data rahasia dengan memasukkan *secret code* terlebih dahulu barulah muncul jumlah *key fragment* yang perlu dimasukkan.


[Home](#)
[Make Secret](#)
[Open Secret](#)

Enter Secret Code

Secret Code

Submit

Key Fragment No. 1

Key Fragment No. 2

Key Fragment No. 3

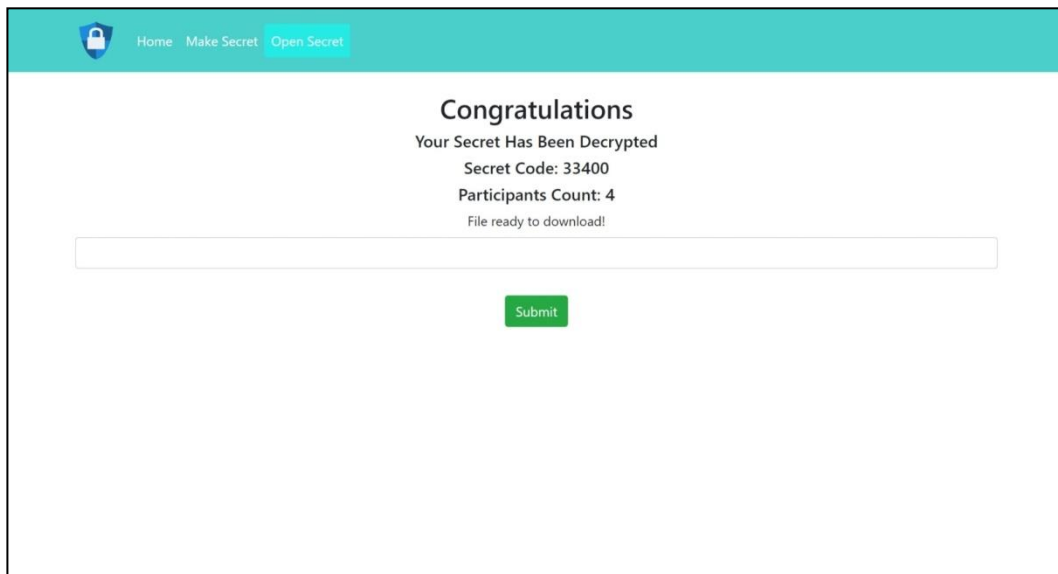
Key Fragment No. 4

Submit

Gambar 4.5 Tampilan Membuka Data Rahasia

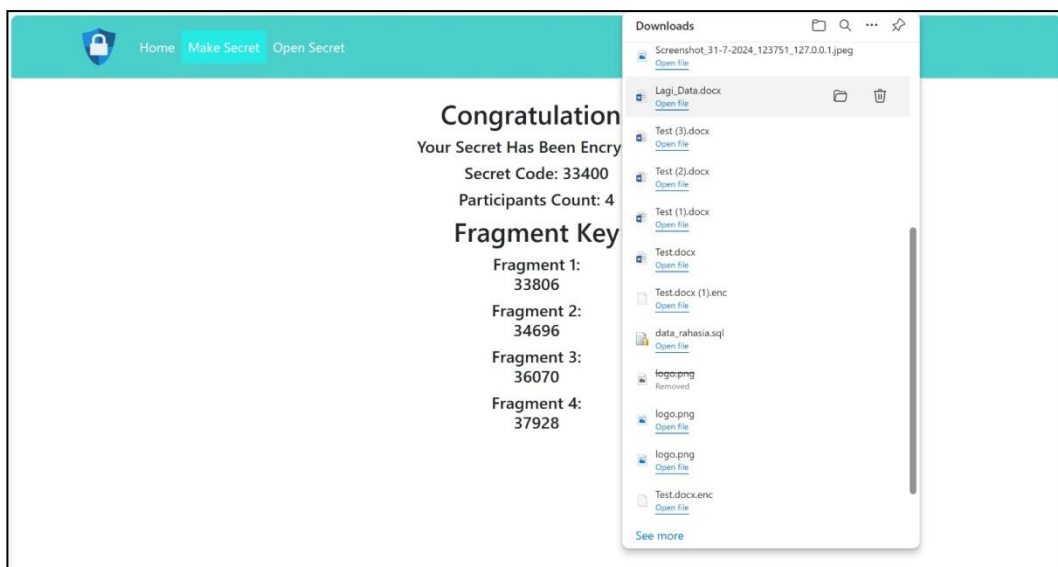
5. Tampilan Berhasil Membuka Data Rahasia.

Tampilan berhasil membuka data rahasia berisikan pesan bahwa data rahasia berhasil dibuka dimana *user* harus memasukkan *pass code* untuk mengunduh dokumen *word* data rahasia.



Gambar 4.6 Tampilan Berhasil Membuka Data Rahasia

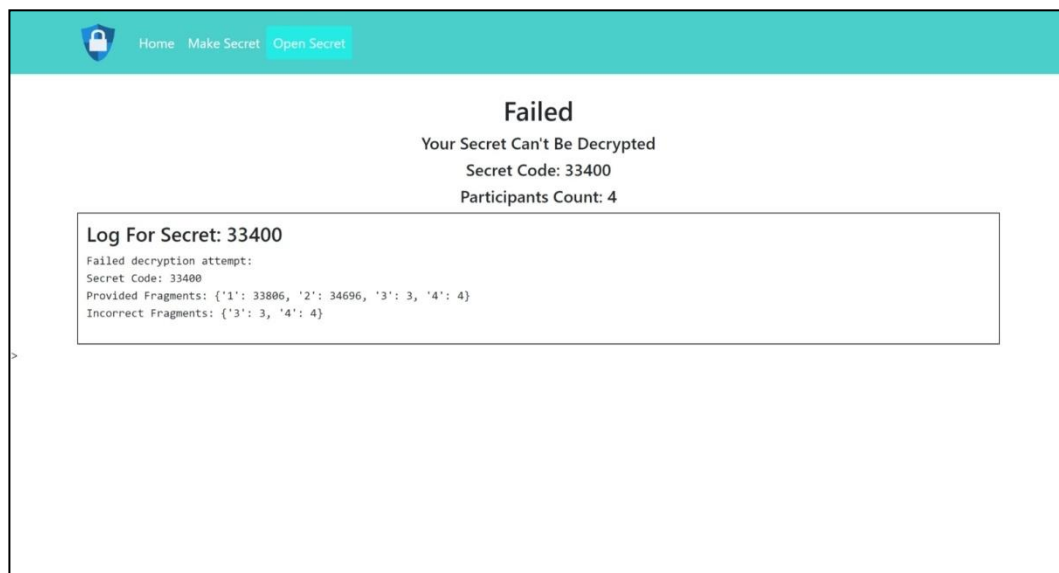
Apabila *pass code* yang dimasukkan sesuai, maka sistem akan otomatis mengunduh data original hasil dekripsi *file*.



Gambar 4.7 File Hasil Dekripsi

6. Tampilan Gagal Membuka Data Rahasia.

Tampilan gagal membuka data rahasia berisikan pesan proses pembukaan data rahasia gagal serta disertakan pesan alasan kegagalan dalam membuka data rahasia tersebut.



Gambar 4.8 Tampilan Gagal Membuka Data Rahasia

4.2 Pembahasan

Pada sub bab ini diuraikan kelebihan dan kekurangan dari *website* layanan pengamanan data rahasia dengan metode enkripsi *Rabin* dan *Shamir Secret Sharing*. Kelebihan dari *website* yang dibangun yaitu:

1. *Website* yang dibangun mengimplementasikan metode enkripsi *Rabin* yang terbukti efektif dalam mengamankan data rahasia. Data yang diunggah dan dienkripsi menjadi tidak dapat diakses oleh pihak yang tidak berwenang.
2. *Website* yang dibangun berhasil menerapkan metode *Shamir Secret Sharing* untuk membagi *ciphertext* menjadi beberapa bagian (*shares*). Hal

ini memungkinkan data rahasia hanya bisa diakses jika sejumlah pecahan kunci yang cukup telah dikumpulkan.

Kekurangan dari *website* yang dibangun yaitu:

1. Panjang pesan rahasia yang dapat diproses oleh sistem dibatasi minimal 1 karakter dan maksimal 10.000 karakter. Hal ini membatasi kemampuan sistem untuk menangani pesan dengan panjang yang lebih besar, yang mungkin diperlukan dalam kasus-kasus tertentu.
2. *Website* ini hanya dapat memproses *file* dengan format *Microsoft Word* (.docx), sehingga tidak dapat digunakan untuk mengamankan data dalam format *file* lain seperti PDF, gambar, atau format dokumen lainnya. Hal ini membatasi fleksibilitas pengguna dalam mengamankan berbagai jenis *file*.
3. *File* hasil pecahan rahasia yang dihasilkan memiliki format khusus (.enc) yang mungkin tidak dikenali oleh pengguna umum. Hal ini menimbulkan kesulitan penggunaan *file-file* pecahan ini di luar sistem yang dibangun.
4. Nilai kunci yang digunakan dalam metode enkripsi Rabin dibatasi antara 2 hingga 6 digit. Batasan ini diberlakukan untuk menjaga agar proses enkripsi dan dekripsi tetap efisien, namun ini juga berarti bahwa kekuatan kunci terbatas dan tidak sekuat yang mungkin dibutuhkan dalam skenario yang memerlukan tingkat keamanan yang lebih tinggi.
5. Sistem membatasi jumlah pecahan rahasia yang dapat dibuat, yaitu antara 2 hingga 100 pecahan. Batasan ini ditetapkan untuk menghindari lamanya waktu proses rekonstruksi, namun membatasi fleksibilitas pengguna dalam menentukan tingkat distribusi kunci yang lebih aman atau sesuai kebutuhan tertentu.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Adapun kesimpulan yang diuraikan berkaitan dengan hasil penelitian yang didapatkan yaitu:

1. *Website* yang dibangun berhasil menerapkan metode enkripsi Rabin secara efektif untuk mengamankan data rahasia. Proses enkripsi ini mengubah pesan asli menjadi *ciphertext* yang tidak dapat dibaca tanpa proses dekripsi yang tepat.
2. *Website* yang dibangun berhasil mengimplementasikan metode *Shamir Secret Sharing* untuk membagi *ciphertext* menjadi beberapa bagian (*shares*). Hal ini memungkinkan pengamanan data rahasia yang lebih kuat karena hanya sebagian dari share yang cukup dapat digunakan untuk merekonstruksi data asli.

5.2 Saran

Berikut ini diuraikan saran untuk dilanjutkan pada penelitian selanjutnya antara lain:

1. Disarankan agar pengembang memperluas dukungan untuk pesan rahasia dengan panjang lebih dari 10.000 karakter. Hal ini akan membuat *website* lebih fleksibel dalam menangani berbagai ukuran pesan rahasia yang mungkin dibutuhkan oleh pengguna.

2. Untuk meningkatkan fleksibilitas dan kegunaan *website*, disarankan untuk menambahkan dukungan untuk berbagai format *file* lainnya, seperti PDF, gambar, dan format dokumen lainnya. Ini akan memungkinkan pengguna untuk mengamankan berbagai jenis data rahasia, bukan hanya *file Microsoft Word*.
3. Agar *file* pecahan rahasia yang dihasilkan lebih mudah digunakan oleh pengguna, disarankan untuk mempertimbangkan format *file* yang lebih umum dikenal atau menyediakan panduan penggunaan yang lebih jelas untuk format *file .enc* yang digunakan.
4. Disarankan untuk memperluas dukungan terhadap nilai kunci *Rabin* yang lebih besar dari 6 digit, dengan tetap memperhatikan efisiensi proses. Ini akan meningkatkan keamanan sistem dan memungkinkan pengguna untuk menyesuaikan tingkat kekuatan kunci sesuai dengan kebutuhan mereka.
5. Untuk lebih meningkatkan fleksibilitas dalam pengamanan data, disarankan agar sistem mendukung jumlah pecahan rahasia yang lebih besar dari 100. Hal ini memungkinkan distribusi kunci yang lebih aman dan adaptasi terhadap kebutuhan skenario tertentu.

DAFTAR PUSTAKA

- [1] W. S. Raharjo, A. Rachmat, and P. Nadirio, "Implementasi Secure Multi-Party Computation Menggunakan Metode Shamir Secret Sharing pada Pengamanan Dokumen Digital Rahasia," *Juisi*, vol. 04, no. 01, pp. 1–9, 2018.
- [2] I. J. Alfreda, R. R. Permata, and T. S. Ramli, "Pelindungan Dan Tanggung Jawab Kebocoran Informasi Pada Penyedia Platform Digital Berdasarkan Perspektif Rahasia Dagang," *J. Sains Sosio Hum.*, vol. 5, no. 1, pp. 1–16, 2021, doi: 10.22437/jssh.v5i1.12767.
- [3] T. H. Subaktiono, "Trend Keamanan Cloud Computing," 2023. [Online]. Available: https://www.researchgate.net/profile/Bayu-Febryan/publication/370097298_Trend_Keamanan_Cloud_Computing/links/643ebefb1b8d044c6331f99f/Trend-Keamanan-Cloud-Computing.pdf.
- [4] M. Afrizal and Y. Reykasari, "Peningkatan Keterampilan Masyarakat Dalam Pengelolaan Dan Penyalinan Arsip Keluarga Secara Digital," *JMM (Jurnal Masy. Mandiri)*, vol. 6, no. 3, p. 2403, 2022, doi: 10.31764/jmm.v6i3.8591.
- [5] A. C. Saputra and A. S. Saragih, "Rancang Bangun Website Badan Pengawas Pemilihan Umum (Bawaslu) Kalimantan Tengah," *J. Teknol. Inf.*, vol. 13, no. 1, pp. 9–17, 2019.
- [6] N. P. Utomo, N. Fahriani, and M. Amirul, "Implementasi Kriptografi Dengan Metode RSA Untuk Keamanan Data Pada Email Berbasis PHP," in *Prosiding-Seminar Nasional Teknologi Informasi & Ilmu Komputer (SEMASTER)*, 2023, vol. 2, no. 1, pp. 97–105.
- [7] D. Hutapea, "Implementasi Algoritma Kriptografi Rabin Dan Lempel-Ziv-Welch (Lzw) Dalam Pengamanan Dan Kompresi File Citra," in *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, 2021, vol. 5, no. 1, pp. 213–220, doi: 10.30865/komik.v5i1.3674.

- [8] C. M. Azzura, M. Pratiwi, and D. Desyanti, "Implementasi Watermarking Desain Citra Menggunakan Metode Modifikasi End of File (Meof)," *JUTEKINF (Jurnal Teknol. Komput. dan Informasi)*, vol. 11, no. 1, pp. 1–9, 2023, doi: 10.52072/jutekinf.v11i1.473.
- [9] Sugianto, Jimmy, A. Suwandhi, Wilianto, and Benny, "Analisis Metode Secret Sharing Asmuth-Bloom Dan Visual Cryptography," *J. Minfo Polgan*, vol. 13, no. 1, pp. 213–218, 2024.
- [10] M. W. R. Pratama, A. Kusyanti, and M. Data, "Implementasi Algoritme Trivium . Stream Cipher Dan Shamir ' s Secret Sharing Pada File Portable Document Format (PDF)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 3, no. 1, pp. 628–633, 2019, [Online]. Available: <http://repository.ub.ac.id/13830/>.
- [11] D. A. Pratiwi, *Artikel Ilmiah Pengantar Sistem Informasi*, no. 43219010158. 2020.
- [12] A. Yoraeni *et al.*, *Sistem Informasi Manajemen*, no. November. Jakarta: PT. Scifintech Andrew Wijaya, 2023.
- [13] N. Azis, *Analisis Perancangan Sistem Informasi*. Bandung: Widina Bhakti Persada, 2022.
- [14] P. E. Sudjiman and L. Siregar, "KOMPUTER DALAM PROSES PENGAMBILAN KEPUTUSAN," *J. TeIKa*, vol. 8, pp. 55–67, 2018.
- [15] R. Ernayani *et al.*, *Dasar dan Teori Sistem Informasi Manajemen*. Batam: Yayasan Cendikia Mulia Mandiri, 2022.
- [16] S. Hidayatullah, D. A. Prasetya, D. A. Purnomo, and I. K. Rachmawati, *Hot Fit Model Pengembangan Sistem Informasi*. Ponorogo: Uwais Inspirasi Indonesia, 2022.
- [17] J. Dalle, A. . Karim, and Baharuddin, *Pengantar Teknologi Informasi*. Depok: PT RajaGrafindo Persada, 2020.
- [18] A. O. Sari, A. Abdilah, and Sunarti, *Web Programming*. Yogyakarta: Graha Ilmu, 2019.
- [19] A. M. Ujung, M. Irwan, and P. Nasution, "Pentingnya Sistem Keamanan Database untuk melindungi data pribadi," *JISKA J. Sist. Inf. Dan Inform.*, vol. 1, no. 2, p. 44, 2023, [Online]. Available:

<http://jurnal.unidha.ac.id/index.php/jteksis>.

- [20] N. Hayaty, *Buku Ajar: Sistem Keamanan*. Riau: Universitas Maritim Raja Ali Haji, 2020.
- [21] R. D. Ardiya and W. Pramusinto, “Implementasi Algoritma Aes-128 Untuk Pengamanan Database Pada Sma Islamic Centre,” in *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, 2022, no. September, pp. 93–102, [Online]. Available: <http://senafiti.budiluhur.ac.id/index.php/senafiti/article/view/120>.
- [22] R. S. Sinaga, S. Purba, and R. M. Siburian, “Aplikasi Pemahaman dan Penerapan Fast (k,n) Threshold Secret Sharing Scheme,” *J. Teknol. Inf. dan Indutri*, vol. 3, no. 1, pp. 76–83, 2023.
- [23] R. A. Sukamto and M. Shalahuddin, “Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek.” Informatika, Bandung, 2018.

DAFTAR RIWAYAT HIDUP

Nama : Steven Alvin Alamsyah
Tempat/Tanggal Lahir : Lubuk Pakam, 28 Maret 2001
Jenis Kelamin : Laki - Laki
Agama : Buddha
Alamat : Jln. KF Tandean No.124
Email : stevenalvin70.sa@gmail.com

Pendidikan Formal :
2007 – 2011 : SD Methodist Lubuk Pakam
2011 – 2013 : SD Swasta Kharisma Tebing Tinggi
2013 - 2016 : SMP Budi Dharma Tebing Tinggi
2016 – 2019 : SMA Swasta F Tandean Tebing Tinggi
2019 - 2024 : STMIK TIME Medan

Medan, 06 Agustus 2024

Steven Alvin Alamsyah



SURAT KEPUTUSAN
NO. 038/SK/P1/STMIKTIME/XII/2023

Tentang
PENGANGKATAN DOSEN PEMBIMBING SKRIPSI
PROGRAM STUDI TEKNIK INFORMATIKA
STMIK TIME

1. **Membaca** : a. Hasil pemeriksaan berkas dan kelengkapan mahasiswa.
b. Presentasi Proposal Judul Skripsi mahasiswa tertanggal 09 Oktober – 18 November 2023.
2. **Mengingat** : a. Kurikulum Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK)Time Program Studi Teknik Informatika.
b. Penyesuaian teknis pelaksanaan Skripsi Program Studi Teknik Informatika.
3. **Menimbang** : Bahwa skripsi mahasiswa merupakan wujud aplikasi kristalisasi sikap kemampuan dan ketrampilan mahasiswa/i dalam upaya menerapkan ilmu pengetahuan yang telah dipelajari dibangku kuliah, serta skripsi merupakan salah satu mata kuliah yang memiliki bobot 6 SKS, maka dipandang perlu untuk menetapkan Dosen Pembimbing I dan Dosen Pembimbing II Skripsi.

4. **Menetapkan** :
Pertama :

Mengangkat Saudara :

Pembimbing I	Robet, M.Kom
Pembimbing II	Hendri, M.Kom

Sebagai Dosen Pembimbing Skripsi atas :

1944074	Steven Alvin Alamsyah	Teknik Informatika
---------	-----------------------	--------------------

Dengan Judul Skripsi :

Perancangan Website Layanan Pengamanan Data Rahasia Dengan Metode Enkripsi Rabin Dan Shamir Secret Sharing
--

Mahasiswa Program Strata Satu (S1) Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK)Time.

- Kedua : Apabila terdapat kekeliruan di kemudian hari tentang penetapan Dosen Pembimbing Skripsi ini akan diperbaiki sebagaimana mestinya
- Ketiga : Surat Keputusan ini berlaku sejak tanggal ditetapkan 07 Desember 2023.

Ditetapkan di
Medan, 07 Desember 2023



Hendri, M.Kom
Pembantu Ketua I STMIK TIME



STMIK TIME

SEKOLAH TINGGI MANAJEMEN INFORMATIKA & KOMPUTER - TIME

FORMULIR BIMBINGAN SKRIPSI

NAMA : STEVEN ALVIN ALAMSYAH
NIM : 1944074
JUDUL SKRIPSI : PERANCANGAN WEBSITE LAYANAN PENGAMANAN DATA RAHASIA DENGAN METODE ENKRIPSI RABIN DAN SHAMIR SECRET SHARING
NAMA DOSEN : ROBET, M.KOM
DOSEN PEMBIMBING : ☒ I (SATU) ☐ II (DUA)

TANGGAL BIMBINGAN	CATATAN BIMBINGAN	PARAF
24 Januari 2024	REVISI BAB I	
05 Februari 2024	ACC BAB I	
14 Maret 2024	REVISI BAB II	
26 April 2024	ACC BAB II	
30 April 2024	REVISI BAB III	
17 Mei 2024	ACC BAB III	
17 Juli 2024	DEMO PROGRAM	
23 Juli 2024	ACC PROGRAM	
29 Juli 2024	REVISI BAB IV	
02 Agustus 2024	ACC BAB IV DAN BAB V	

Ketentuan :

1. Bimbingan dengan dosen pembimbing minimal 8 (delapan) kali
2. Formulir Bimbingan wajib diisi dan ditunjukkan ke dosen pembimbing tiap bimbingan
3. Formulir Bimbingan Skripsi ini dianggap sah, apabila telah mendapatkan Pengesahan dari dosen pembimbing
4. Jika tidak memenuhi ketentuan di atas, skripsi dapat **DIBATALKAN**

Medan, 02 Agustus 2024

Dosen Pembimbing,



ROBET, M.KOM

Mahasiswa,

STEVEN ALVIN ALAMSYAH



STMIK TIME

SEKOLAH TINGGI MANAJEMEN INFORMATIKA & KOMPUTER - TIME

FORMULIR BIMBINGAN SKRIPSI

NAMA : STEVEN ALVIN ALAMSYAH
NIM : 1944074
JUDUL SKRIPSI : PERANCANGAN WEBSITE LAYANAN PENGAMANAN DATA RAHASIA DENGAN METODE ENKRIPSI RABIN DAN SHAMIR SECRET SHARING
NAMA DOSEN : HENDRI, M.KOM
DOSEN PEMBIMBING : ☐ I (SATU) ☒ II (DUA)

TANGGAL BIMBINGAN	CATATAN BIMBINGAN	PARAF
27 Februari 2024	Revisi Bab 1, Penjelas Bagian Sistematika Penulisan	
23 April 2024	Bab 1 Acc	
26 April 2024	Bab 2 Acc	
18 Mei 2024	Bab 3 Acc, Ajukan ke Semprom	
05 Agustus 2024	Rapikan Bab 4 dan 5	
06 Agustus 2024	Bab 4 dan 5 Acc, Lengkapi Dokumen Skripsi dan Paper	
08 Agustus 2024	Acc Final, Ajukan ke Sidang Meja Hijau	

Ketentuan :

1. Bimbingan dengan dosen pembimbing minimal 8 (delapan) kali
2. Formulir Bimbingan wajib diisi tiap bimbingan
3. Formulir Bimbingan Skripsi ini dianggap sah, apabila telah mendapatkan Pengesahan dari dosen pembimbing
4. Jika tidak memenuhi ketentuan di atas, skripsi dapat **DIBATALKAN**

Medan, 08 Agustus 2024

Dosen Pembimbing,



Hendri, M.Kom

Mahasiswa,

Steven Alvin Alamsyah

LISTING PROGRAM