SKRIPSI

PENGAMANAN DATA PADA BASIS DATA MENGGUNAKAN *SEARCHABLE ENCRYPTION* DENGAN KUNCI SIMETRI

ALVIN IRAWAN

NPM: 2013730001

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS
UNIVERSITAS KATOLIK PARAHYANGAN

2017

UNDERGRADUATE THESIS

DATA SECURITY IN THE DATABASE USING SEARCHABLE ENCRYPTION WITH SYMMETRY KEY

ALVIN IRAWAN

NPM: 2013730001

DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND SCIENCES
PARAHYANGAN CATHOLIC UNIVERSITY
2017

LEMBAR PENGESAHAN

PENGAMANAN DATA PADA BASIS DATA MENGGUNAKAN *SEARCHABLE ENCRYPTION* DENGAN KUNCI SIMETRI

ALVIN IRAWAN

NPM: 2013730001

Bandung, 18 Mei 2017

Menyetujui,

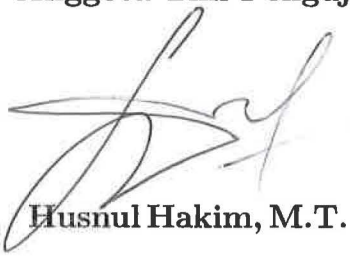
Pembimbing

Mariskha Tri Adithia, P.D.Eng

Ketua Tim Penguji

Luciana Abednego, M.T.

Anggota Tim Penguji



Husnul Hakim, M.T.

Mengetahui,

Ketua Program Studi

Mariskha Tri Adithia, P.D.Eng

PERNYATAAN

Dengan ini saya yang bertandatangan di bawah ini menyatakan bahwa skripsi dengan judul:

PENGAMANAN DATA PADA BASIS DATA MENGGUNAKAN *SEARCHABLE ENCRYPTION* DENGAN KUNCI SIMETRI

adalah benar-benar karya saya sendiri, dan saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan.

Atas pernyataan ini, saya siap menanggung segala risiko dan sanksi yang dijatuhkan kepada saya, apabila di kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya, atau jika ada tuntutan formal atau non-formal dari pihak lain berkaitan dengan keaslian karya saya ini.

Dinyatakan di Bandung,
Tanggal 18 Mei 2017

Alvin Irawan
NPM: 2013730001

ABSTRAK

Enkripsi sering kali digunakan untuk melakukan pengamanan data. Penambahan keamanan dengan mengenkripsi data tersebut membuat entitas yang tidak berkepentingan tidak dapat mengetahui apapun dari data tersebut. Aktivitas ini baik untuk menjaga kerahasiaan, namun merugikan pada saat melakukan pencarian terhadap data tersebut. Salah satu cara melakukan pencarian adalah mendekripsi seluruh data lalu dilakukan pencarian. Untuk mengatasi masalah ini, diajukan cara melakukan enkripsi baru yaitu *searchable encryption* dengan memakai kunci simetri.

Searchable encryption dengan kunci simetri adalah algoritma *searchable encryption* yang memakai kunci yang sama untuk proses enkripsi dan juga dekripsi. Sebelum data dienkripsi, setiap data diberikan kata kunci, lalu data dan kata kunci tersebut dienkripsi dan disimpan. Proses pencarian dilakukan dengan cara mencari kata kunci yang sesuai. Proses dekripsi akan dilakukan terhadap hasil pencarian apabila ditemukan kata kunci yang sesuai.

Hasil yang diperoleh dari algoritma *searchable encryption* dengan memakai kunci simetri ini adalah *ciphertext* yang dapat dicari. *Ciphertext* ini lebih baik dari *ciphertext* hasil enkripsi lainnya karena dapat dilakukan pencarian dan tetap menjaga kerahasiaan data. Durasi pencarian pada algoritma ini berdasarkan metode pencarian yang dikemukakan oleh Dawn Song [1] sudah lebih cepat dibandingkan dengan mendekripsi seluruh *ciphertext* lalu dilakukan pencarian.

Berdasarkan pengujian yang didapatkan dari perangkat lunak yang telah dibangun, algoritma *searchable encryption* dengan memakai kunci simetri ini dapat diterapkan pada basis data. Proses pencarian pada algoritma ini dapat dibuat lebih cepat dengan cara mencari hasil enkripsi dari kata kunci langsung ke dalam basis data.

Kata-kata kunci: *searchable encryption*, *searchable encryption* dengan kunci simetri, *ciphertext*

ABSTRACT

Encryption is often used to secure data. The addition of security by encrypting the data leaves the unauthenticated entity unable to know anything from the data. This activity is good for maintaining confidentiality, but is harmful when searching for the data. One way to search is to decrypt all data and then search. To solve this problem, it is proposed a new way to encrypt the data using searchable encryption with symmetry key.

Searchable encryption with symmetry key is the algorithm of searchable encryption which uses the same key for the encryption process as well as the decryption. Before data is encrypted, each data is given a keyword, then the data and keywords are encrypted and stored. The search process is done by searching for the appropriate keywords. The decryption process will be made to the search results when the appropriate keywords are found.

The result obtained from the searchable encryption algorithm with symmetry key is searchable ciphertext. This ciphertext is better than ciphertext of other encryption as it can be searched and keep the data confidentiality. The search duration of this algorithm based on the search method proposed by Dawn Song [1] is faster than decrypting all ciphertext and then doing the searching.

Based on the tests obtained from the software that has been built, the searchable encryption with symmetry key algorithm can be applied to the database. The searching process of this algorithm can be made faster by searching the encryption of keywords directly into the database.

Keywords: *searchable encryption*, symmetric key searchable encryption, ciphertext

Dipersembahkan untuk orang tua tercinta..

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya penulis berhasil menyusun skripsi dengan judul "Pengamanan Data pada Basis Data menggunakan *Searchable Encryption* dengan Kunci Simetri". Penulis menyadari bahwa penyusunan skripsi ini tidak terlepas dari bantuan dan dukungan berbagai pihak. Oleh karena itu penulis ingin mengucapkan terima kasih kepada:

- Kedua orang tua yang selalu memberikan dukungan untuk menyelesaikan skripsi ini.
- Kakak penulis, Caecilia yang menjadi *proof-reader* dan penyedia UltraMilk rasa stroberi.
- Dosen pembimbing, Bu Mariskha yang memberikan bimbingan, masukan, dan tambahan wawasan selama proses pembuatan skripsi ini sehingga selesai dengan baik.
- Anggota Bacoters, Adrian Rey-cheater-naldi, Enricofindley ga pake spasi, Fransiskus Evanub, Harkosseto Pandityo, Alinna Belalai Margareta, Ke-vinA-ntonius, yang menyediakan hiburan dan hobi mengajak kompe CS:GO saat sedang menyusun skripsi.
- Tim Geladi Diri Lembaga Pengembangan Humaniora, Mba Aty, Mba Ria, Mas YB, Pak Sosro, serta teman-teman asisten yang membantu untuk melatih diri dan menjadi rekan kerja yang baik.
- Staf dan teman-teman magang pada Pusat Pengembangan Karir yang telah memberikan kesempatan untuk bekerja sama dalam 6 bulan terakhir.

Semoga seluruh pihak yang membantu dalam penyusunan skripsi ini mendapat berkah dah rahmat dari Tuhan Yang Maha Esa. Akhir kata, penulis memohon maaf bila terdapat kesalahan dan kekurangan dalam penyusunan skripsi ini. Semoga skripsi ini berguna bagi semua pihak yang membutuhkan.

Bandung, Mei 2017

Penulis

DAFTAR ISI

Kata Pengantar xv

Daftar Isi xvii

Daftar Gambar xix

Daftar Tabel xxi

1 Pendahuluan 1
- 1.1 Latar Belakang . . . 1
- 1.2 Rumusan Masalah . . . 2
- 1.3 Tujuan . . . 2
- 1.4 Batasan Masalah . . . 2
- 1.5 Metodologi . . . 3
- 1.6 Sistematika Pembahasan . . . 3

2 Landasan Teori 5
- 2.1 Kriptografi . . . 5
- 2.2 Fungsi Hash . . . 6
- 2.3 Jaringan Feistel . . . 6
- 2.4 *Data Encryption Standard* . . . 7
- 2.5 *Rivest cipher 4* . . . 9
- 2.6 FJ-RC4 . . . 10
- 2.7 Siphash . . . 10
- 2.8 *Searchable Encryption* . . . 12

3 Analisis 15
- 3.1 Analisis Masalah . . . 15
- 3.2 FJRC4 Untuk Kunci DES . . . 16
- 3.3 Enkripsi dengan algoritma DES . . . 18
- 3.4 Pembuatan *Mask* Sebelah kiri . . . 20
- 3.5 Pembuatan *Mask* Sebelah Kanan . . . 20
- 3.6 Enkripsi dengan Algoritma *Searchable Encryption* dengan kunci simetri . . . 22
- 3.7 Pencarian Data . . . 22
  - 3.7.1 Pencarian menurut Dawn Song . . . 22
  - 3.7.2 Pencarian usulan . . . 23
- 3.8 Dekripsi Data . . . 23
- 3.9 Analisis Kebutuhan Perangkat Lunak . . . 23
  - 3.9.1 Penyimpanan Data . . . 24
  - 3.9.2 Pencarian Data Menurut Dawn Song . . . 25
  - 3.9.3 Pencarian Data Usulan . . . 26
- 3.10 Diagram Aktivitas . . . 27
- 3.11 Diagram Hubungan Entitas . . . 29

3.12 Diagram Kelas 30

4 Perancangan **35**
4.1 Perancangan Antarmuka 35
4.2 Perancangan basis data 38
4.3 Perancangan Kelas 40
4.4 Deskripsi dan Fungsi Setiap Kelas 40
4.4.1 Kelas UI 40
4.4.2 Kelas EngineUI 41
4.4.3 Kelas Controller 41
4.4.4 Kelas Engine 41
4.4.5 Kelas PRP_DES 48
4.4.6 Kelas PRNG_FJRC4 52
4.4.7 Kelas PRF_Siphash 55
4.4.8 Kelas dbConnector 56
4.4.9 Kelas Converter 57

5 Implementasi dan Pengujian Perangkat Lunak **59**
5.1 Tampilan Antarmuka Perangkat Lunak 59
5.1.1 Tampilan awal 59
5.1.2 Tampilan Penambahan Data 60
5.1.3 Tampilan Pencarian Data 61
5.2 Pengujian Perangkat Lunak 63
5.2.1 Pengujian Fungsional 63
5.2.2 Pengujian Eksperimental 67
5.2.3 Kesimpulan Pengujian 70

6 Kesimpulan dan Saran **71**
6.1 Kesimpulan 71
6.2 Saran 71

Daftar Referensi **73**

A Tabel Des **75**

DAFTAR GAMBAR

2.1 Jaringan Feistel . . . 7
2.2 Diagram enkripsi DES . . . 9
2.3 Skema dasar *Searchable Encryption* . . . 12
2.4 Skema perbaikan *Searchable Encryption* . . . 13
2.5 Skema pencarian *Searchable Encryption* . . . 13
2.6 Skema final *Searchable Encryption* . . . 14

3.1 *Flowchart* penyelesaian masalah . . . 24
3.2 *Flowchart* proses enkripsi dan penyimpanan data . . . 24
3.3 *Flowchart* proses pencarian oleh Dawn Song . . . 25
3.4 *Flowchart* proses pencarian data usulan . . . 26
3.5 Diagram aktivitas proses enkripsi . . . 27
3.6 Diagram aktivitas proses dekripsi . . . 28
3.7 Diagram aktivitas pencarian data 1 . . . 28
3.8 Diagram aktivitas pencarian data 2 . . . 29
3.9 Diagram hubungan entitas . . . 29

4.1 Halaman antarmuka awal . . . 35
4.2 Halaman antarmuka tambah data . . . 36
4.3 Halaman antarmuka untuk penampilan pesan . . . 36
4.4 Halaman antarmuka "Lihat Data Mahasiswa" . . . 37
4.5 Halaman antarmuka "Lihat Data Universitas" . . . 37
4.6 Halaman antarmuka "Lihat Semua Data" . . . 37
4.7 Diagram kelas rinci . . . 39
4.8 Kelas UI . . . 40
4.9 Kelas EngineUI . . . 41
4.10 Kelas Controller . . . 41
4.11 Kelas Engine . . . 41
4.12 Kelas PRP_DES . . . 48
4.13 Kelas PRNG_FJRC4 . . . 53
4.14 Kelas PRF_Siphash . . . 55
4.15 Kelas dbConnector . . . 56
4.16 Kelas Converter . . . 57

5.1 Halaman antarmuka awal . . . 59
5.2 Halaman antarmuka penambahan data . . . 60
5.3 Pesan bila data tidak lengkap . . . 60
5.4 Pesan bila data bherhasil dimasukkan . . . 60
5.5 Halaman antarmuka pencarian data mahasiswa . . . 61
5.6 Halaman antarmuka pencarian data universitas . . . 62
5.7 Halaman antarmuka pencarian data gabungan . . . 62
5.8 Halaman antarmuka bila pencarian data berhasil . . . 62
5.9 Halaman antarmuka bila pencarian data gagal . . . 63

5.10 Tabel bio dan tabel univ kosong 64
5.11 Penambahan data "Sekar" 64
5.12 Tabel bio dan univ setelah penambahan satu data 65
5.13 Tabel bio dan univ setelah penambahan tiga data 65
5.14 Hasil pencarian dengan kata kunci "Bandung" 66
5.15 Hasil pencarian dengan kata kunci "Mobil" 66
5.16 Hasil pencarian dengan kata kunci "Mobil, Bandung" 67
5.17 Hasil pencarian dengan kata kunci "Unpar" 67
5.18 Perbandingan kecepatan pencarian 17-1.088 data 69
5.19 Perbandingan kecepatan pencarian 8074-557.056 data 70

DAFTAR TABEL

2.1 Permutasi Awal 7

3.1 Nilai awal array 16
3.2 Nilai awal array $s0$ pada pengulangan pertama 16
3.3 Nilai awal array $s0$ pada pengulangan kedua 17
3.4 Nilai awal array $s0$ pada pengulangan ke-255 17
3.5 Nilai awal array $s1$ pada pengulangan ke-255 17
3.6 Nilai awal array $s2$ pada pengulangan ke-255 17
3.7 Nilai array setelah pembuangan sekian nilai pertama 18
3.8 Nilai hasil setelah pembuangan sekian nilai pertama 18
3.9 Nilai hasil operasi XOR 18
3.10 Nilai array setelah pembuangan sekian nilai pertama 20
3.11 Nilai hasil operasi XOR 20
3.12 Tabel bio 30
3.13 Tabel Univ 30
3.14 Atribut kelas UI 30
3.15 Atribut kelas EngineUI 30
3.16 Atribut kelas Controller 31
3.17 Atribut kelas Engine 31
3.18 Atribut kelas PRP_DES 32
3.19 Atribut kelas PRF_Siphash 32
3.20 Atribut kelas PRNG_FJRC4 33
3.21 Atribut kelas DbConnector 33

4.1 Tabel bio 38
4.2 Tabel Univ 38

5.1 Data yang akan digunakan 63
5.2 Data yang digunakan untuk percobaan eksperimental 68
5.3 Hasil percobaan perbandingan kecepatan metode pencarian dan dekripsi dalam satuan detik 69

A.1 Permutasi Awal 75
A.2 Inversi Permutasi Awal 75
A.3 Permutasi Ekspansi 75
A.4 *P-Box* 75
A.5 *Permutation Choice - 1* 75
A.6 *Permutation Choice - 2* 75
A.7 *S-Box* ke-1 76
A.8 *S-Box* ke-2 76
A.9 *S-Box* ke-3 76
A.10 *S-Box* ke-4 76
A.11 *S-Box* ke-5 76

A.12 *S-Box* ke-6 76
A.13 *S-Box* ke-7 76
A.14 *S-Box* ke-8 76

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Kriptologi adalah ilmu yang mempelajari mengenai kode. Kriptologi terbagi menjadi 2 bagian [2], kriptografi yang mempelajari mengenai pembuatan kode, dan *cryptanalysis* yang mempelajari pemecahan kode. Tujuan utama dari kriptografi adalah menjaga kerahasiaan, menjaga integritas, dan melakukan otentikasi. Dalam kriptografi terdapat 2 istilah mengenai suatu data atau informasi, yaitu *plaintext* dan *ciphertext*. *Plaintext* (terkadang disebut *cleartext*) adalah data atau informasi yang belum dienkripsi atau sudah didekripsi, dan *ciphertext* adalah *plaintext* yang sudah dienkripsi. Kriptografi yang umumnya digunakan sekarang ini dibagi menjadi tiga kategori berdasarkan jumlah kunci yang dipakai untuk melakukan proses enkripsi dan proses dekripsi. Salah satu dari ketiga kategori tersebut adalah kriptografi kunci simetri yang hanya memakai satu buah kunci untuk proses enkripsi dan dekripsi. Contoh dari kriptografi kunci simetri ini adalah algoritma *Data Encryption Standard* (DES).

Dewasa ini, pada umumnya media penyimpanan data beragam, mulai dari dicatat atau ditulis di kertas sampai disimpan pada *cloud server*. Selain media, pengolahan data sebelum disimpan juga dapat dibedakan menjadi 2, yaitu dicatat begitu saja (*plaintext*) atau diamankan dengan cara dienkripsi terlebih dahulu (*ciphertext*). Pencatatan data dengan cara dienkripsi terlebih dahulu memiliki kelebihan dan kekurangan. Kelebihannya adalah data yang disimpan menjadi lebih aman karena pihak yang tidak berkepentingan sulit untuk membacanya. Kekurangan dari cara ini adalah sulitnya untuk mencari sebagian dari data tersebut. Untuk melakukan pencarian perlu dilakukan proses dekripsi terlebih dahulu. Proses dekripsi pada umumnya bersifat *all-or-nothing*, yaitu *ciphertext* dapat didekripsi seluruhnya menjadi *plaintext* atau tidak sama sekali. Sifat ini menjadi tidak baik jika diterapkan untuk penyimpanan data pada basis data. Sebagai contoh, dengan menggunakan algoritma enkripsi AES dengan kunci "asd" dan panjang 128 bit, hasil enkripsi dari "FTIS UNPAR" adalah "KNL4OYY0BSnJUM7xtxbeSg==". Terdapat 2 pilihan ketika akan dicari data yang mengandung kata "FTIS", yaitu mendekripsikan seluruh isi basis data atau mencari hasil enkripsi dari kata "FTIS". Penggunaan cara mendekripsikan seluruh isi basis data pasti akan mengembalikan hasil, namun cara ini menghabiskan waktu yang semakin lama dengan semakin banyaknya jumlah data. Penggunaan cara mencari hasil enkripsi tidak akan membuahkan hasil karena hasil enkripsi (dengan algoritma dan kunci yang sama, AES - "asd") dari kata "FTIS" adalah "g8wLFxIzthsRuePquDP9og==".

Selain kelebihan dan kekurangan secara umum seperti yang sudah dijelaskan, jenis kriptografi yang digunakan juga mempengaruhi keamanan data yang dienkripsi. Jenis yang dimaksud adalah kriptografi kunci simetri dan kriptografi kunci asimetri. Kriptografi kunci simetri memakai satu kunci untuk proses enkripsi dan juga proses dekripsi. Kriptografi kunci asimetri memakai kunci yang berbeda untuk proses enkripsi dan proses dekripsi. Penggunaan kriptografi kunci asimetri lebih aman dibandingkan dengan memakai kunci simetri karena bila terjadi kebocoran mengenai kunci untuk proses enkripsi, data yang dienkripsi tetap aman karena tidak dapat didekripsi dengan kata kunci tersebut.

Pada skripsi ini, akan dibahas mengenai salah satu cara melakukan enkripsi menggunakan

algoritma *Searchable Encryption* dengan kunci simetri. Algoritma *Searchable Encryption* ini akan membuat pencarian lebih aman karena hanya sebagian dari *ciphertext* yang dikirimkan untuk melakukan proses pencarian. Dalam membangun algoritma ini, dibutuhkan beberapa algoritma lainnya untuk menghasilkan *pseudo-random number generator*, *pseudo-random permutation*, dan *pseudo-random function*. *Pseudo-random number generator*[1] adalah pembangkit nilai-nilai yang terlihat acak berdasarkan pada nilai masukan. *Pseudo-random function*[2] adalah fungsi untuk menghasilkan nilai acak. *Pseudo-random number generator* dan *pseudo-random function* sekilas terlihat mirip namun sebetulnya berbeda. Hasil dari *pseudo-random number generator* berupa sebuah rangkaian nilai acak yang digunakan secara terurut berdasarkan urutan dalam rangkaian, sementara *pseudo-random function* mengambil nilai dalam rangkaian tersebut dengan cara yang terlihat acak. *Pseudo-random permutation*[3] adalah fungsi $F : K \times D \rightarrow D$ (dengan $K = \{0,1\}^k$, dan $D = \{0,1\}^l$, untuk k dan $l \geq 1$)dimana hasil dari masukan dan keluarannya tidak dapat dibedakan secara perhitungan dengan nilai permutasi acak pada D. Dalam penggunaannya, algoritma enkripsi *Searchable Encryption* dengan kunci simetri ini secara umum dapat menerima masukan dalam bentuk apapun. Teks, gambar, audio, atau bentuk *file* lainnya tidak terkecuali. Untuk melakukan pencarian pada algoritma ini memerlukan masukan seperti apa yang dienkripsi pada saat memasukan data. Selain pembahasan mengenail hal-hal yang sudah disebutkan, pad skripsi ini juga dibuat sebuah perangkat lunak yang mengimplentasikan algoritma *Searchable Encryption* dengan kunci simetri.

1.2 Rumusan Masalah

Rumusan masalah yang akan dibahas dalam penelitian ini :

1. Bagaimana cara kerja *Searchable Encryption* dengan kunci simetri untuk basis data?
2. Bagaimana implementasi *Searchable Encryption* dengan kunci simetri untuk basis data?

1.3 Tujuan

Tujuan yang ingin dicapai dalam penelitian ini :

1. Mempelajari cara kerja *Searchable Encryption* dengan kunci simetri untuk basis data
2. Mengimplementasikan *Searchable Encryption* dengan kunci simetri untuk basis data dengan menggunakan bahasa pemrograman Java

1.4 Batasan Masalah

Batasan-batasan masalah yang diterapkan dalam penelitian ini adalah :

1. Masukan yang diterima hanyalah huruf, angka, dan tanda baca.
2. Pencarian bersifat *case sensitive* (sesuai dengan saat disimpan).

[1]Ben Lynn, "Pseudo-Random Number Generators",diakses dari https://crypto.stanford.edu/pbc/notes/crypto/prng.html, 23 April 2017 pukul 16:00 WIB

[2]Ben Lynn,"Pseudo-Random Functions", diakses dari https://crypto.stanford.edu/pbc/notes/crypto/prf.html, 23 April 2017 pukul 16:05 WIB

[3]Ben Lynn, "Pseudo-Random Permutations",diakses dari https://crypto.stanford.edu/pbc/notes/crypto/prp.html, 23 April 2017 pukul 16:15 WIB

1.5 Metodologi

Metodologi yang digunakan untuk menyusun penelitian ini adalah sebagai berikut:

1. Melakukan studi pustaka mengenai kriptografi terutama bagian *Searchable Encryption*. Studi pustaka ini juga mempelajari algoritma lainnya yang digunakan dalam membangun algoritma *Searchable Encryption* dengan kunci simetri yaitu algoritma DES, algoritma FJRC4, dan algoritma Siphash.
2. Melakukan analisis perangkat lunak.
3. Membuat perancangan antarmuka dan diagram kelas perangkat lunak.
4. Membangun perangkat lunak yang mengimplementasikan *Searchable Encryption* dengan kunci simetri.
5. Melakukan pengujian terhadap hasil implementasi *Searchable Encryption* terhadap beberapa contoh kasus.
6. Menarik kesimpulan berdasarkan hasil pengujian.

1.6 Sistematika Pembahasan

Sistematika pembahasan dibagi menjadi beberapa bab yang dijelaskan sebagai berikut:

1. Bab 1 Pendahuluan
   Bab pendahuluan membahas mengenai latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi, dan sistematika pembahasan.
2. Bab 2 Dasar Teori
   Bab dasar teori membahas mengenai teori-teori dasar kriptografi, DES, FJRC4, siphash, dan *Searchable Encryption*
3. Bab 3 Analisis
   Bab analisis membahas masalah yang dihadapi dan solusi yang dapat menyelesaikannya, studi kasus, pengembangan *Searchable Encryption*, dan perancangan perangkat lunak.
4. Bab 4 Perancangan
   Bab perancangan membahas mengenai diagram kelas rinci, deskripsi dan fungsi dari setiap kelas yang dibangun, kebutuhan keluaran dan masukan dari perangkat lunak, dan perancangan antarmuka perangkat lunak.
5. Bab 5 Implementasi dan Pengujian Perangkat Lunak
   Bab ini membahas mengenai tampilan dari perangkat lunak yang dibangun, pengujian dari perangkat lunak, dan kesimpulan dari hasil pengujian
6. Bab 6 Kesimpulan dan Saran
   Bab ini membahas mengenai kesimpulan dari penelitian ini serta saran untuk pengembangannya lebih lanjut.