

**KOMBINASI ALGORITMA BEAUFORT CHIPER DAN HILL
CHIPER DALAM MENGAMANKAN FILE DOKUMEN
BERBASIS MOBILE**

SKRIPSI

MUHAIMI RIZKI SIREGAR

07011731195



**PROGRAM STUDI ILMU KOMPUTER
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA
MEDAN**

2022

**KOMBINASI ALGORITMA BEAUFORT CHIPER DAN HILL
CHIPER DALAM MENGAMANKAN FILE DOKUMEN
BERBASIS MOBILE**

SKRIPSI

Diajukan untuk Memenuhi Syarat Mencapai Gelar Sarjana Komputer

MUHAIMI RIZKI SIREGAR

07011731195



**PROGRAM STUDI ILMU KOMPUTER
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA
MEDAN
2022**

Persetujuan Skripsi

Hal : Surat Persetujuan Skripsi
Lampiran : -

Kepada Yth,
Dekan Fakultas Sains dan Teknologi
Universitas Islam Negeri Sumatera Utara Medan

Assalamua'laikum Warahmatullahi Wabarakatuh.

Setelah membaca, meneliti, memberikan petunjuk, dan mengoreksi serta mengadakan perbaikan, kami selaku pembimbing berpendapat bahwa skripsi saudara,

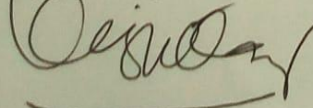
Nama : Muhaimi Rizki Siregar
Nomor Induk Mahasiswa : 0701173195
Program Studi : Ilmu Komputer
Judul : Kombinasi Algoritma Beaufort Chiper Dan Hill
Chiper Dalam Mengamankan File Dokumen
Berbasis Mobile

Dapat disetujui untuk segera dimunaqasyahkan. Atas perhatiannya kami ucapkan terimakasih.

Medan, 05 September 2022
08 Safar 1444 H

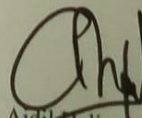
Komisi pembimbing,

Pembimbing Skripsi 1



Heri Santoso, M. Kom
NIP.1100000114

Pembimbing Skripsi 2



Aidil Halim Lubis M. Kom
NIP.198805272019031010



KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA MEDAN
FAKULTAS SAINS DAN TEKNOLOGI

Jl. Lapangan Golf, Desa Durian Jangak, Kecamatan Pancur Batu,
Kabupaten Deli Serdang Provinsi Sumatera Utara, Kode Pos 20353
Website : <https://www.saintek.uinsu.ac.id> E-mail : saintek@uinsu.ac.id

PENGESAHAN SKRIPSI

Nomor : B.197/ST/ST.V.2/PP.01.1/09/2022

Judul : Kombinasi Algoritma Beaufort Chiper Dan Hill
Chiper Dalam Mengamankan File Dokumen
Berbasis Mobile

Nama : Muhaimi Rizki Siregar

Nomor Induk Mahasiswa : 07011731195

Program : Ilmu Komputer

Fakultas : Sains dan Teknologi

Telah dipertahankan dihadapan Dewan Penguji Skripsi Program Studi Fisika
Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara Medan
dan dinyatakan **LULUS**.

Pada hari/ tanggal : Selasa / 23 September 2022

Tempat : Ruang Sidang Fakultas Sains dan Teknologi

Tim Ujian Munaqasyah,
Ketua,

Ilka Zufria, S.Kom., M.Kom
NIP. 198506042015031006
Dewan Penguji,

Penguji I,

Yusuf Ramadnan Nasution, M.Kom
NIP 198505252023211025

Penguji II,

Rakhmat Kurniawan R, M.Kom
NIP 198503162015031003

Penguji III,

Heri Santoso, M. Kom
NIP. 196711192023211002

Penguji IV,

Aidil Halim Lubis M. Kom
NIP 198805272019031010

Mengesahkan,
Dekan Fakultas Sains dan Teknologi
UIN Sumatera Utara Medan



Dr. Mhd. Syahnun, M.A.
NIP. 196609051991031002

SURAT PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan dibawah ini:

Nama	: Muhaimi Rizki Siregar Nomor
Induk Mahasiswa	: 07011731195
Program Studi	: Ilmu Komputer
Judul	: Kombinasi Algoritma Beaufort Chiper Dan Hill Chiper Dalam Mengamankan File Dokumen Berbasis Mobile

Menyatakan bahwa skripsi ini adalah hasil karya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya. Apabila di kemudian hari ditemukan plagiat dalam skripsi ini maka saya bersedia menerima sanksi pencabutan gelar akademik yang saya peroleh dan sanksi lainnya sesuai dengan peraturan yang berlaku.

Medan, 05 Agustus 2022

Muhaimi Rizki Siregar
NIM. 07011731195

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

KATA PENGANTAR

Assalamu Alaikum Wr.Wb

Segala puji dan syukur penulis ucapkan kehadirat Allah SWT. Yang telah melimpahkan rahmat, hidayah dan karunianya pada penulis sehingga penulis dapat menyelesaikan skripsi yang berjudul “Kombinasi Algoritma Beaufort Chiper Dan Hill Chiper Dalam Mengamankan File Dokumen Berbasis Mobile”. Tak lupa shalawat beriring salam penulis hadiahkan kepada baginda Nabi Muhammad SAW yang telah membawa kita kealam terang benderang yang diridhai Allah SWT dan selalu kita syafaatkan di yaumul akhir kelak.

Pada kesempatan ini penulis juga mengucapkan terimakasih atas segala bantuan yang diberikan baik moril maupun materil secara langsung maupun tidak langsung sehingga penulisan skripsi ini bisa diselesaikan. Disini penulis dengan segala kerendahan hati mengucapkan terimakasih yang sebesar-besarnya kepada :

1. Bapak Prof Dr.Syahrin Harahap, M.A, selaku Rektor UIN Sumatera Utara yang telah memberikan kesempatan untuk menimba ilmu di lembaga yang beliau pimpin.
2. Bapak Dr. Mhd. Syahnan, MA, selaku Dekan Fakultas Sains Dan Teknologi UIN Sumatera Utara.
3. Bapak Ilka Zufria, M.Kom, selaku Ketua Program Studi Ilmu Komputer, Fakultas Sains Dan Teknologi.
4. Bapak Rakhmat Kurniawan R, S.T., M.Kom, selaku Sekretaris Program Studi Ilmu Komputer.
5. Bapak Heri Santoso, M.Kom, selaku dosen pembimbing I yang telah berkontribusi membantu penulis dalam memberikan ide, saran, kritik, motivasi, dan bimbingan kepada penulis selama penulis mengerjakan skripsi.

6. Bapak Aidil Halim Lubis, M.Kom, selaku dosen pembimbing II yang telah berkontribusi membantu penulis dalam memberikan ide, saran, kritik, motivasi, dan bimbingan kepada penulis selama penulis mengerjakan skripsi.
7. Bapak Armansyah, M.Kom, sebagai dosen pembimbing akademik yang telah berkontribusi membantu penulis dalam memberikan bimbingannya selama masa perkuliahan.
8. Teristimewa ucapan terima kasih kepada kedua orang tua tercinta, yaitu Ayah penulis H. Mukmin Siregar dan Ibu Hj. Nurisam Harahap yang telah memberikan bantuan moril maupun materil, semangat dan doa yang begitu besar kepada penulis yang tidak terbalas jasanya.
9. Seluruh tenaga pengajar dan pegawai program studi S1 Ilmu Komputer maupun Fakultas Sains dan Teknologi UIN Sumatera Utara.
10. Teman-teman kelas Ilmu Komputer 5 terkhusus kepada, Ayu Sahriani, Multi Dana, Aisatun Siregar, Nida Khofiyya, Hazizah Ulfa, Winny Wiyandari, Wan Ilia Fitri dan Lely Damanik yang selalu memberikan dukungan kepada penulis.
11. Saudara-saudari penulis dan Empat Serangkai atas doa dan kasih sayang yang selalu tercurah selama ini. Dan semua pihak yang telah membantu penulis namun tidak dapat disebutkan satu persatu.

Akhir kata penulis mengucapkan terimakasih kepada seluruh pihak yang turut membantu dan semoga skripsi ini dapat bermanfaat bagi kita semua. Semoga Allah SWT. Selalu melimpahkan rahmat, hidayah dan karuniaNya kepada kita semua. Aamiin.

Medan, 08 Agustus 2022

Hormat Saya

Muhaimi Rizki Siregar

NIM.0701173195

ABSTRAK

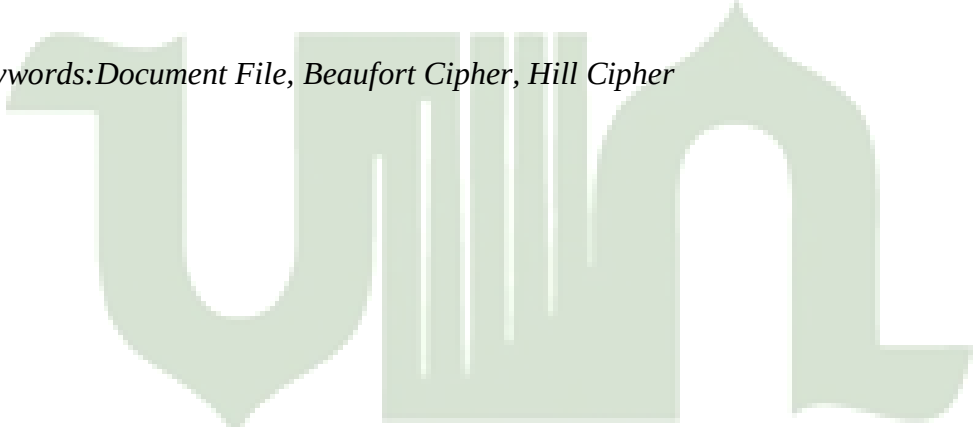
Penelitian ini bertujuan untuk mengamankan suatu *file* dokumen yang memiliki informasi yang bersifat rahasia atau pribadi. Sehingga dibutuhkan suatu sistem yang dapat digunakan untuk mengamankan *file* dokumen sehingga tidak dapat diakses oleh orang lain yang tidak berkepentingan. Pengamanan *file* dokumen dilakukan menggunakan kombinasi algoritma *beaufort cipher* dan *hill cipher*. *Beaufort cipher* adalah salah satu varian dari *vigenère cipher* dimana cara melakukan enkripsi dan dekripsi hampir sama dengan melakukan enkripsi dan dekripsi pada *vigenère cipher*. *Hill Cipher* merupakan salah satu algoritma kriptografi yang memanfaatkan matriks sebagai kunci untuk melakukan enkripsi dan dekripsi dari aritmatika modulo. Langkah awal pengamanan dilakukan menggunakan algoritma *Beaufort Cipher* selanjutnya hasil pengamanan algoritma *Beaufort Cipher* diamankan kembali menggunakan *Hill Cipher*. Prose pengamanan dilakukan menggunakan 4 buah kunci dikarenakan *Hill Cipher* menggunakan perkalian matrix 2x2. Hasil akhir dari penelitian ini merupakan sebuah aplikasi berbasis android yang dapat digunakan dalam proses pengamanan *file* dokumen dengan ekstensi .docx, .xlsx dan .pdf. *File* dokumen yang telah diamankan akan memiliki ekstensi .mhi sebagai penanda bagi peneliti. Dokumen yang telah diamankan dapat dikembalikan ke dalam bentuk aslinya menggunakan aplikasi yang telah dihasilkan pada penelitian ini menggunakan kunci yang sama digunakan dalam proses pengamanan.

Kata kunci : File Dokumen, Beaufort Cipher, Hill Cipher

ABSTRACT

This study aims to secure a document file that has confidential or private information. So we need a system that can be used to secure document files so that they cannot be accessed by unauthorized persons. Document file security is carried out using a combination of the Beaufort cipher and hill cipher algorithms. Beaufort cipher is a variant of the vigenre cipher where the encryption and decryption method is almost the same as encrypting and decrypting the vigenre cipher. Hill Cipher is a cryptographic algorithm that uses a matrix as a key to encrypt and decrypt modulo arithmetic. The initial step of security is carried out using the Beaufort Cipher algorithm, then the results of the Beaufort Cipher algorithm are secured again using Hill Cipher. The security process is carried out using 4 keys because Hill Cipher uses a 2x2 matrix multiplication. The final result of this research is an android-based application that can be used in the process of securing document files with .docx, .xlsx and .pdf extensions. Document files that have been secured will have an .mhi extension as a marker for researchers. Documents that have been secured can be returned to their original form using the application that has been generated in this study using the same key used in the security process.

Keywords: Document File, Beaufort Cipher, Hill Cipher



UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

DAFTAR ISI

	Halaman
ABSTRAK	i
ABSTRACT	ii
Daftar isi	iii
Daftar Tabel.....	iv
Daftar Gambar	v
BAB I PENDAHULUAN	1
1.1.Latar Belakang	1
1.2.Rumusan Masalah	3
1.3.Batasan Masalah.....	3
1.4.Tujuan Penelitian	3
1.5.Manfaat Penelitian.....	4
BAB II TINJAUAN PUSTAKA	5
2.1.Kriptografi	5
2.1.1.Jenis Kriptografi	7
2.1.2.Keamanan Data	8
2.1.3.Aspek Keamanan Data.....	8
2.1.4.Perkembangan Kriptografi.....	10
2.2.Algoritma Beaufort Cipher	10
2.3.Algoritma Hill Cipher.....	11
2.4.Dokumen.....	14
2.5.Flowchart.....	15
2.6.Pemrograman Java	16
2.7.Android	17
2.8. Versi Android.....	19
2.9. Android Studio.....	20
2.10.Android SDK (<i>Software Development Kit</i>)	20
BAB III METODOLOGI PENELITIAN.....	22
3.1.Waktu dan Jadwal Penelitian.....	22
3.2.Bahan dan Alat Penelitian	22
3.2.1. Perangkat Keras.....	22
3.2.2. Perangkat Lunak	23

3.3.Cara Kerja.....	23
3.3.1. Perencanaan.....	23
3.3.1.1. <i>Flowchart</i> Enkripsi.....	23
3.3.1.2. <i>Flowchart</i> Dekripsi	25
3.3.2. Teknik Pengumpulan Data.....	26
3.3.3. Metode Penelitian.....	26
3.3.3.1. Analisis Kebutuhan	27
3.3.3.2. Desain Sistem.....	28
3.3.3.3. Implementasi.....	28
3.3.3.4. Pengujian	28
3.3.3.5. Pengembangan	28
BAB IV HASIL DAN PEMBAHASAN	30
4.1 Pembahasan.....	30
4.1.1 Analisa Data	30
4.1.2. <i>Flowchart</i> Sistem.....	35
4.1.2.1 <i>Flowchart</i> Menu Enkripsi Dokumen	35
4.1.2.2 <i>Flowchart</i> Menu Deskripsi Dokumen.....	36
4.1.2.3 <i>Flowchart</i> Menu Tentang Aplikasi	36
4.1.3.Desain Antarmuka	37
4.2 Hasil.....	41
4.1.1 Pengujian Aplikasi	41
4.1.2Hasil Pengujian Aplikasi	45
BAB V KESIMPULAN DAN SARAN.....	48
5.1 Kesimpulan	48
5.2 Saran.....	49
DAFTAR PUSTAKA	

DAFTAR GAMBAR

2.1 Algoritma Kriptografi Simetri	7
2.2 Algoritma Kriptografi Asimetri	8
3.1 <i>Flowchart</i> Enkripsi	24
3.2 <i>Flowchart</i> Dekripsi	25
3.3 Model Waterfall Metode Penelitian	27
4.1 <i>Flowchart</i> Menu Enkripsi Dokumen	35
4.2 <i>Flowchart</i> Menu Deskripsi Dokumen	36
4.3 <i>Flowchart</i> Menu Tentang Aplikasi	37
4.4 Desain Halaman Utama.....	38
4.5 Desain Halaman Enkripsi File Dokumen	39
4.6 Desain Halaman Deskripsi File Dokumen	40
4.7 Desain Halaman Tentang Aplikasi	41
4.8 Tampilan Halaman Utama.....	42
4.9 Tampilan Halaman Enkripsi Dokumen.....	43
4.10 Tampilan Halaman Deskripsi Dokumen	44
4.11 Tampilan Halaman Tentang Aplikasi	45

DAFTAR TABEL

2.1 Simbol-simbol <i>Flowchart</i>	15
2.2 Versi-versi Android.....	19
3.1 Waktu dan Jadwal Penelitian.....	22
4.1 Himpunan Karakter Algoritma Beaufort Chiper	31
4.2 Himpunan Karakter Algoritma Hill Chiper.....	32
4.3 Hasil Pengujian Aplikasi	46

