

**IMPLEMENTASI KOMBINASI ALGORITMA *BEAUFORT*  
*CIPHER* DAN ALGORITMA RSA DALAM SKEMA  
SUPER ENKRIPSI UNTUK PENGAMANAN  
*FILE* TEKS**

**SKRIPSI**



**PROGRAM STUDI ILMU KOMPUTER  
FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA  
MEDAN  
2023**

**IMPLEMENTASI KOMBINASI ALGORITMA *BEAUFORT*  
*CIPHER* DAN ALGORITMA RSA DALAM SKEMA  
SUPER ENKRIPSI UNTUK PENGAMANAN  
*FILE* TEKS**

**SKRIPSI**

*Diajukan untuk Memenuhi Syarat Mencapai Gelar Sarjana Komputer*



**MAHYUDI  
0701162010**



UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN  
UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN

**PROGRAM STUDI ILMU KOMPUTER  
FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA  
MEDAN  
2023**

## PERSETUJUAN SKRIPSI

Hal : Surat Persetujuan Skripsi

Lamp : -

Kepada Yth.,

Dekan Fakultas Sains dan Teknologi

Universitas Islam Negeri Sumatera Utara Medan

*Assalamu'alaikum Wr. Wb.*

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

Nama	: Mahyudi
NIM	: 0701162010
Program Studi	: Ilmu Komputer
Judul	: Implementasi Kombinasi Algoritma <i>Beaufort Cipher</i> dan Algoritma RSA dalam Skema Super Enkripsi untuk Pengamanan <i>File</i> Teks.

dapat disetujui untuk segera *dimunaqasyahkan*. Atas perhatiannya kami ucapkan terimakasih.

Medan, 20 Februari 2023 M  
29 Rajab 1444 H

UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN

Komisi Pembimbing,

Pembimbing Skripsi I,



Yusuf Ramadhan Nst, M.Kom  
NIB. 1100000075

Pembimbing Skripsi II,



Abdul Halim Hasugian, M.Kom  
NIB. 1100000113

## SURAT PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan dibawah ini :

Nama : MAHYUDI  
Nomor Induk Mahasiswa : 0701162010  
Program Studi : Ilmu Komputer  
Judul Skripsi : Implementasi Kombinasi Algoritma  
*Beaufort Cipher* dan Algoritma RSA dalam  
Skema Super Enkripsi untuk Pengamanan  
*File Teks*

Dengan ini menyatakan skripsi ini adalah hasil karya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya. Apabila dikemudian 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, Februari 2023



UNIVERSITAS IS  
SUMATERA UTARA MEDAN

Mahyudi  
NIM.0701162010

**PENGESAHAN SKRIPSI**

Nomor : B.154/ST/ST.V.2/PP.01.1/05/2023

Judul : Implementasi Kombinasi Algoritma *Beaufort Cipher*  
dan Algoritma RSA dalam Skema Super Enkripsi  
untuk Pengamanan *File* Teks  
Nama : Mahyudi  
Nomor Induk Mahasiswa : 0701162010  
Program Studi : Ilmu Komputer  
Fakultas : Sains Dan Teknologi

Telah dipertahankan dihadapan Dewan Penguji Skripsi Program Studi Ilmu Komputer  
Fakultas Sains dan Teknologi UIN Sumatera Utara Medan dan dinyatakan **LULUS**.

Pada hari/tanggal : Senin, 27 Februari 2023  
Tempat : Ruang Meeting Fakultas Sains dan Teknologi UIN  
Sumatera Utara Medan, Kampus IV- Tuntungan

Tim Ujian Munaqasyah,  
Ketua,

Ilka Zufria, M.Kom  
NIP.198506042015031006

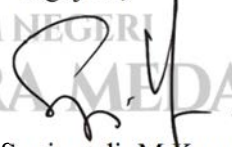
Dewan Penguji,

Penguji I,



Ilka Zufria, M.Kom  
NIP. 198506042015031006

Penguji II,



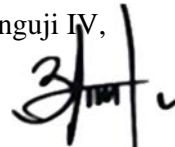
Supiyandi, M.Kom  
NIB. 0701209006

Penguji III,



Yusuf Ramadhan Nasution, M.Kom  
NIB. 1100000075

Penguji IV,



Abdul Halim Hasugian, M.Kom  
NIB. 1100000113

Mengesahkan,  
Dekan Fakultas Sains dan Teknologi  
UIN Sumatera Utara Medan.

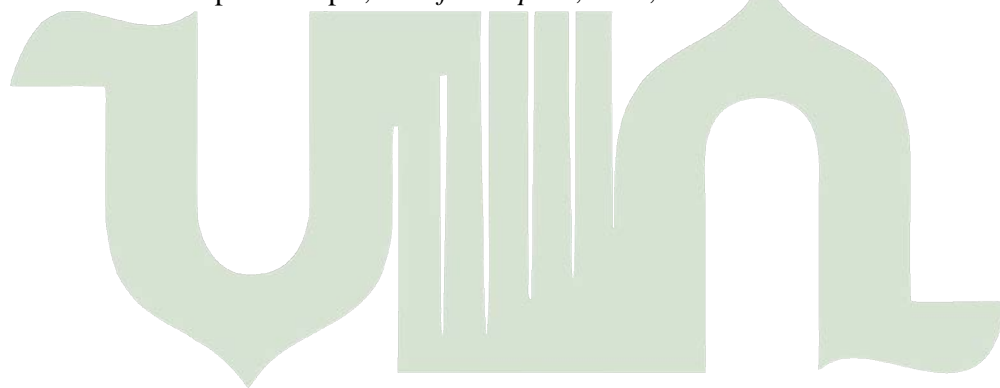


Prof. Dr. Mhd Syahnan, M.A.  
NIP. 196609051991031002

## ABSTRAK

Kriptografi merupakan salah satu alternatif solusi yang dapat diterapkan untuk menjaga dan meningkatkan keamanan data. Pada penelitian ini akan mengimplementasikan perpaduan algoritma kriptografi simetris *Beaufort Cipher* dan algoritma kriptografi asimetris RSA dalam skema super enkripsi guna meningkatkan keamanan data pada *file* teks. Kombinasi dua algoritma kriptografi dilakukan dengan cara mengenkripsi pesan yang terdapat dalam *file* teks terlebih dahulu menggunakan kunci algoritma *Beaufort Cipher*, kemudian mengenkripsi kembali dengan kunci publik algoritma RSA untuk menghasilkan *file* teks terenkripsi. Metode pengkombinasian antara kedua algoritma bertujuan untuk mendapatkan hasil enkripsi (*ciphertext*) yang lebih kuat sehingga tidak mudah untuk dipecahkan, dan juga untuk mengatasi penggunaan *ciphertext* tunggal yang secara komparatif lemah karena hanya menggunakan satu algoritma kriptografi. Penelitian ini menghasilkan sebuah aplikasi berbasis web yang dapat digunakan untuk mengamankan *file* teks dengan menggunakan kombinasi algoritma *Beaufort Cipher* dan algoritma RSA dalam skema super enkripsi.

**Kata Kunci** : Super Enkripsi, *Beaufort Cipher*, RSA, *File* Teks

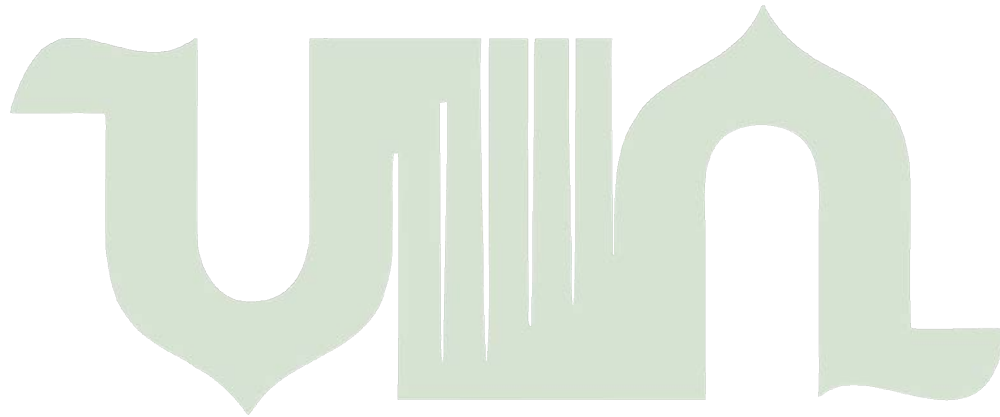


UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN

## ABSTRACT

Cryptography is an alternative solution that can be applied to maintain and improve data security. This research will implement a combination of the Beaufort Cipher symmetric cryptographic algorithm and the RSA asymmetric cryptographic algorithm in a super encryption scheme to increase data security in text files. The combination of the two cryptographic algorithms is done by first encrypting the message contained in the text file using the Beaufort Cipher algorithm key, then re-encrypting it with the public key of the RSA algorithm to produce an encrypted text file. The combination method between the two algorithms aims to get stronger encryption (ciphertext) results so that it is not easy to crack, and also to overcome the use of a single ciphertext which is comparatively weak because it only uses one cryptographic algorithm. This research produces a web-based application that can be used to secure text files using a combination of the Beaufort Cipher algorithm and the RSA algorithm in a super encryption scheme.

**Keyword** : Super Encryption, Beaufort Cipher, RSA, Text Files



UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN

## KATA PENGANTAR

*Bismillahirrahmanirrahim. Alhamdulillah* rabbi 'alamin, sebelumnya tidak lupa penulis ucapkan puji dan syukur atas kehadiran Allah Subhanahu Wa Ta'ala yang telah memberikan rahmat dan karunia-Nya kepada penulis sehingga penulis diberikan kesempatan untuk dapat menyelesaikan skripsi dengan judul "Implementasi Kombinasi Algoritma *Beaufort Cipher* dan Algoritma RSA dalam Skema Super Enkripsi untuk Pengamanan *File* Teks". Adapun skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan program Strata-1 di Jurusan Ilmu Komputer, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara, Medan.

Penulis menyadari dalam penyelesaian skripsi ini tidak terlepas dari bantuan dan dukungan banyak pihak, sehingga dengan penuh rasa hormat penulis ingin mengucapkan terima kasih yang sebesar-besarnya bagi semua pihak yang telah membantu di mana terdapat bantuan moril serta materil yang sangat berguna dalam proses penyelesaian proposal skripsi ini, terutama kepada :

1. Bapak Prof. Dr. Abu Rokhmad, M.Ag, selaku Plt. Rektor Universitas Islam Negeri Sumatera Utara Medan.
2. Bapak Prof. Dr. Mhd. Syahnan, M.A, selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara Medan.
3. Bapak Ilka Zufria, M.Kom, selaku Ketua Program studi Ilmu Komputer Universitas Islam Negeri Sumatera Utara Medan.
4. Bapak Rakhmat Kurniawan R, S.T., M.Kom, selaku Sekretaris Program Studi Ilmu Komputer Universitas Islam Negeri Sumatera Utara Medan.
5. Bapak Yusuf Ramadhan Nasution, M.Kom, selaku Dosen Pembimbing I
6. Bapak Abdul Halim Hasugian, M.Kom, selaku Dosen Pembimbing II
7. Bapak Dr. Mhd. Furqan, S.Si., M.Comp.Sc, selaku Dosen Pembimbing Akademik.
8. Bapak/ibu dosen dan staff di lingkungan Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara Medan, khususnya pada Program Studi Ilmu Komputer.



9. Seluruh teman-teman yang selalu memberikan dukungan kepada penulis.
10. Dan terakhir yang paling istimewa yaitu kepada kedua orang tua penulis yang senantiasa selalu memberikan dukungan disertai doa dan juga bantuan-bantuan lainnya yang tidak dapat disebutkan satu persatu yang membuat penulis semakin semangat dalam penyelesaian skripsi ini.

Dalam penulisan skripsi ini, penulis menyadari bahwa sepenuhnya masih jauh dari kata sempurna dikarenakan terbatasnya pengalaman dan pengetahuan yang dimiliki penulis. Untuk itu, penulis berharap kepada pembaca untuk dapat memberikan sumbangsih pikiran berupa kritik dan saran yang membangun.

Akhir kata penulis mengucapkan terima kasih kepada semua pihak yang telah ikut membantu dalam penyelesaian skripsi ini, dan penulis berharap skripsi ini nantinya dapat bermanfaat bagi semua pihak di masa mendatang.



Medan, Februari 2023  
Penulis,  
  
Mahyudi  
NIM. 0701162010

UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN

## DAFTAR ISI

	Halaman
<b>ABSTRAK .....</b>	<b>i</b>
<b>ABSTRACT .....</b>	<b>ii</b>
<b>KATA PENGANTAR.....</b>	<b>iii</b>
<b>DAFTAR ISI.....</b>	<b>v</b>
<b>DAFTAR GAMBAR.....</b>	<b>viii</b>
<b>DAFTAR TABEL .....</b>	<b>x</b>
<b>DAFTAR LAMPIRAN.....</b>	<b>xi</b>
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah .....	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian.....	5
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>6</b>
2.1 Kriptografi .....	6
2.1.1 Super Enkripsi .....	8
2.2 Sistem Kriptografi ( <i>Cryptosystem</i> ).....	8
2.2.1 <i>Symmetric Cryptosystem</i> .....	9
2.2.2 <i>Asymmetric Cryptosystem</i> .....	9
2.3 Algoritma <i>Beaufort Cipher</i> .....	10
2.4 Algoritma RSA.....	14
2.4.1 Pembangkit Kunci Algoritma RSA .....	15
2.4.2 Proses Enkripsi Algoritma RSA .....	18

2.4.3 Proses Dekripsi Algoritma RSA.....	19
2.5 <i>File</i> Teks.....	19
2.6 <i>Flowchart</i> .....	21
<b>BAB III METODE PENELITIAN .....</b>	<b>22</b>
3.1 Tempat dan Waktu Penelitian .....	22
3.1.1 Tempat Penelitian .....	22
3.1.2 Waktu & Jadwal Pelaksanaan Penelitian.....	22
3.2 Bahan dan Alat Penelitian .....	23
3.2.1 Perangkat Keras .....	23
3.2.2 Perangkat Lunak .....	23
3.3 Cara Kerja.....	24
3.3.1 Perencanaan .....	24
3.3.2 Teknik Pengumpulan Data.....	28
3.3.3 Analisis Kebutuhan.....	29
3.3.3.1 Analisis Kebutuhan Fungsional .....	29
3.3.3.2 Analisis Kebutuhan Non Fungsional .....	30
3.3.4 Perancangan .....	31
3.3.4.1 <i>Flowchart</i> Sistem .....	31
3.3.4.2 Rancangan <i>Interface</i> Sistem.....	36
3.3.5 Pengujian .....	37
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>	<b>39</b>
4.1 Analisis Penerapan Metode .....	39
4.1.1 Analisis Proses Enkripsi .....	39
4.1.2 Analisis Proses Dekripsi .....	47
4.2 Perancangan Sistem.....	52

4.2.1 Perancangan Halaman Utama.....	52
4.2.2 Perancangan Halaman Bangkitkan Kunci .....	53
4.2.3 Perancangan Halaman Enkripsi.....	54
4.2.4 Perancangan Halaman Dekripsi.....	54
4.2.5 Perancangan Halaman <i>Help</i> .....	55
4.2.6 Perancangan Halaman <i>About</i> .....	56
4.3 Implementasi Program .....	56
4.3.1 Implementasi Halaman Utama.....	57
4.3.2 Implementasi Halaman Bangkitkan Kunci.....	57
4.3.3 Implementasi Halaman Enkripsi.....	58
4.3.4 Implementasi Halaman Dekripsi .....	59
4.3.5 Implementasi Halaman <i>Help</i> .....	59
4.3.6 Implementasi Halaman <i>About</i> .....	60
4.4 Hasil Pengujian.....	61
4.4.1 Hasil Pengujian Bangkitkan Kunci.....	61
4.4.2 Hasil Pengujian Enkripsi .....	63
4.4.3 Hasil Pengujian Dekripsi .....	65
4.4.4 Hasil Pengujian <i>Black box Testing</i> .....	66
<b>BAB V KESIMPULAN DAN SARAN.....</b>	<b>71</b>
5.1 Kesimpulan.....	71
5.2 Saran.....	71
<b>DAFTAR PUSTAKA .....</b>	<b>72</b>
<b>LAMPIRAN-LAMPIRAN</b>	

## DAFTAR GAMBAR

Gambar	Judul Gambar	Halaman
2.1	Gambaran Umum Proses Enkripsi dan Dekripsi .....	7
2.2	Skema <i>Symmetric Cryptosystem</i> .....	9
2.3	Skema <i>Asymmetric Cryptosystem</i> .....	10
2.4	Enkripsi <i>Beaufort Cipher</i> Teknik <i>Tabula Recta</i> .....	12
3.1	Tahapan Penelitian .....	25
3.2	Arsitektur Umum Sistem .....	27
3.3	<i>Flowchart</i> Sistem Halaman Utama .....	32
3.4	<i>Flowchart</i> Sistem Halaman Bangkitkan Kunci .....	33
3.5	<i>Flowchart</i> Sistem Halaman Enkripsi .....	34
3.6	<i>Flowchart</i> Sistem Halaman Dekripsi .....	35
4.1	Skema Proses Enkripsi .....	40
4.2	Potongan Sampel Data .....	40
4.3	Potongan Sampel Data (a) Karakter (b) Nilai Desimal .....	41
4.4	Skema Proses Dekripsi .....	47
4.5	Rancangan <i>Interface</i> Halaman Utama .....	53
4.6	Rancangan <i>Interface</i> Halaman Bangkitkan Kunci .....	53
4.7	Rancangan <i>Interface</i> Halaman Enkripsi .....	54
4.8	Rancangan <i>Interface</i> Halaman Dekripsi .....	55
4.9	Rancangan <i>Interface</i> Halaman <i>Help</i> .....	55
4.10	Rancangan <i>Interface</i> Halaman <i>About</i> .....	56
4.11	Tampilan Halaman Utama .....	57
4.12	Tampilan Halaman Bangkitkan Kunci .....	58

4.13	Tampilan Halaman Enkripsi .....	58
4.14	Tampilan Halaman Dekripsi .....	59
4.15	Tampilan Halaman <i>Help</i> .....	60
4.16	Tampilan Halaman <i>About</i> .....	60
4.17	Hasil Pengujian Bangkitkan Kunci .....	62
4.18	Hasil Kunci Algoritma RSA (a) Kunci Publik (b) Kunci Privat .....	62
4.19	Hasil Pengujian Enkripsi <i>Beaufort Cipher</i> .....	63
4.20	Hasil Pengujian Enkripsi RSA .....	64
4.21	Hasil Pengujian Dekripsi RSA .....	65
4.22	Hasil Pengujian Dekripsi <i>Beaufort Cipher</i> .....	66



UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN

## DAFTAR TABEL

<b>Tabel</b>	<b>Judul Tabel</b>	<b>Halaman</b>
2.1	Proses Enkripsi <i>Beaufort Cipher</i> Teknik <i>Tabula Recta</i> .....	12
2.2	Tabel Substitusi Angka Algoritma <i>Beaufort Cipher</i> .....	13
2.3	Proses Substitusi Angka <i>Beaufort Cipher</i> .....	13
2.4	Simbol-simbol <i>Flowchart</i> .....	21
3.1	Jadwal Pelaksanaan Penelitian.....	22
4.1	Proses Mengubah <i>Plaintext</i> Menjadi Desimal .....	42
4.2	Perbandingan Hasil Enkripsi.....	47
4.3	Konversi Desimal Kedalam Tabel ASCII.....	49
4.4	Proses Mengubah <i>Ciphertext1</i> Menjadi Desimal .....	50
4.5	<i>Black box Testing</i> Bangkitkan Kunci.....	67
4.6	<i>Black box Testing</i> Enkripsi .....	68
4.7	<i>Black box Testing</i> Dekripsi .....	69

UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN

## DAFTAR LAMPIRAN

Lampiran	Judul Lampiran
1.	Listing Program
2.	Daftar Riwayat Hidup
3.	Kartu Bimbingan Skripsi



UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN