

**IMPLEMENTASI ALGORITMA DATA ENCRYPTION STANDART (DES) UNTUK
PENGAMANAN DATA PADA DOKUMEN PDF**

SKRIPSI



UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

ARIF WIJAYA PANJAITAN

NIM. 0701163093

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

**IMPLEMENTASI ALGORITMA DATA ENCRYPTION STANDART (DES) UNTUK
PENGAMANAN DATA PADA DOKUMEN PDF**

SKRIPSI

Diajukan Untuk Memenuhi Syarat Mencapai Gelar Sarjana komputer



UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

ARIF WIJAYA PANJAITAN

NIM. 0701163093

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

2022

PERSETUJUAN SKRIPSI

Hal : Surat Persetujuan Skripsi

Lamp : -

Kepada Yth.,
Dekan Fakultas Sains dan Teknologi
UIN Sumatera Utara Medan

Assalamu'alaikum Wr. Wb

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

Nama : ARIF WIJAYA PANJAITAN
Nomor Induk Mahasiswa : 0701163093
Program Studi : Ilmu komputer
Judul : Implementasi Algoritma DataEncryption Standard (DES)
Untuk Pengamanan Data Pada Dokumen PDF

Dapat disetujui untuk segera di*Munaqasyahkan*. Atas perhatiannya kami ucapkan terimakasih.

Medan, 10 Maret 2021
26 Rajab 1442 H

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN
Komisi Pembimbing,

Pembimbing I,



Ilka zufria, M.Kom.
NIP. 198506042015031006

Pembimbing II,

Yusuf Ramadhan Nasution, M.Kom
NIB. 1100000075

Saya yang bertanda tangan di bawah ini

Nama : ARIF WIJAYA PANJAITAN

Nomor Induk Mahasiswa :0701163093

Program Study :Ilmu Komputer

Judul :Implementasi Algoritma DataEncryption Standard (DES) Untuk
Pengamanan Data Pada Dokumen PDF

Dengan ini menyatakan bahwa skripsi ini adalah hasil karya sendiri,kecuali beberapa kutipan dan ringkasann yang masing masing di sebutkan 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.

Lubuk Pakam,21 april 2022


ARIF WIJAYA PANJAITAN
NIM.0701163093

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN



KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA MEDAN
FAKULTAS SAINS DAN TEKNOLOGI
JL. IAIN No. 1 Medan 20235
Telp. (061) 6615683-6622925, Fax. (061) 6615683
Url: <http://saintek.uinsu.ac.id>, E-mail: saintek@uinsu.ac.id

PENGESAHAN SKRIPSI

Nomor: B.299/ST/ST.V.2/PP.01.1/11/2022

Judul : Implementasi Algoritma Data Encryption Standart (DES) Untuk Pengamanan Data Pada Dokumen PDF

Nama : ARIF WIJAYA PANJAITAN

Nomor Induk Mahasiswa : 0701163093

Program Studi : Ilmu Komputer

Fakultas : Sains dan Teknologi

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

Pada hari/tanggal : Rabu, 27 April 2022

Tempat Media : Ruang H.202 Gedung Kuliah Bersama H. Anif, Kampus I- Sutomo

Tim Ujian Munaqasyah,
Ketua,

Ilka Zufria, M.Kom.
NIP. 198506042015031006

Dewan Penguji,

Penguji I,

Ilka Zufria, M.Kom.
NIP. 198506042015031006

Penguji II,

Yusuf Ramadhan Nasution, M.Kom.
NIB. 1100000075

Penguji III,

Rakhmat Kurniawan, R. M.kom.
NIP. 198503162015031003

Penguji IV,

Sriani, M.Kom.
NIB. 1100000108

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



Prof. Dr. Ang. Syahnan, M.A
NIP. 196409051991031002

ABSTRAK

Penyalahgunaan dan pencurian dokumen PDF yang bersifat rahasia, karena dokumen masih dapat dikenali dan dibaca oleh manusia, dan tentunya hal tersebut merugikan pihak yang memiliki akses terhadap data dokumen PDF tersebut. Dengan menerapkan teknik enkripsi kriptografi, penyadapan dan pencurian dokumen PDF dapat diminimalkan. Kriptografi adalah ilmu yang mempelajari teknik matematika yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, dan otentikasi.

Kriptografi membutuhkan algoritma untuk melakukan proses enkripsi, dan salah satu algoritma kriptografi yang dapat digunakan adalah algoritma Data Encryption Standard (DES). Algoritma DES adalah algoritma simetris berdasarkan prinsip block cipher. Algoritma DES menggunakan kunci 64-bit untuk mengenkripsi blok dan 64 bit. Artikel ini membahas perancangan kriptografi berbasis web dengan menggunakan metode Data Encryption Standard (DES). Implementasi pada sistem ini menggunakan kunci 8 digit untuk menyembunyikan file pdf tanpa error atau kerusakan file dan tidak dapat didekripsi tanpa kunci yang tepat. Menggunakan sistem aplikasi keamanan data yang menggunakan metode DES bermanfaat untuk membantu menyembunyikan isi file pdf penting dengan kunci, sehingga meminimalkan pencurian digital oleh orang yang tidak bertanggung jawab.

Kata Kunci : kriptografi, Data encryption Standard, Portable Dokument Format

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

ABSTRACT

Misuse and theft of confidential PDF documents because documents can still be recognized and read by humans means, of course, these problems can harm those who have access to PDF document data. The act of tapping and stealing PDF documents can be minimized by the application of cryptographic encryption techniques. Cryptography is a science that studies mathematical techniques related to information security aspects such as confidentiality, data integrity and authentication. Cryptography requires an algorithm to perform the encryption process, one of the cryptographic algorithms that can be used is the Standard Data Encryption (DES) algorithm. The DES algorithm is a symmetric algorithm that works on the principle of a block cipher. The DES algorithm uses a 64-bit key to encrypt a 64-bit block. This thesis discusses the design of web-based cryptography using the Data Encryption Standard (DES) method. The application of this system is hiding pdf files using an 8-bit key without any errors or file damage and cannot be decrypted without the appropriate key. By using a data security application system using the DES method, it is useful to help hide the contents of important pdf files with a key so as to minimize digital theft by irresponsible parties.

Keywords : kriptografi , Data encryption Standart, Portable Dokument Format

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Segala puji dan syukur penulis panjatkan ke hadirat Allah SWT, karena dengan izin-Nya penulis dapat menyelesaikan makalah ini. Shalawat dan salam semoga senantiasa tercurah kepada Nabi besar Muhammad SAW.

Disertasi ini dimaksudkan untuk melengkapi dan memenuhi syarat menjalankan program mata kuliah Strata-1 di Universitas Islam Negeri Sumatera Utara semester 8 Ilmu Komputer. Dalam proses penulisan makalah ini, penulis sangat menyadari keterbatasan, kemampuan dan wawasannya sendiri, dan menerima pendapat dan saran yang berharga dari semua pihak.

Penulis banyak menemui kesulitan dalam proses penulisan, namun dengan bimbingan dan bantuan dari berbagai pihak akhirnya penulis dapat menyelesaikan skripsi yang berjudul : ***“Implementasi Algoritma DataEncryption Standart (DES) Untuk Pengamanan Data Pada Dokumen PDF”***.

Demi kelancaran dalam penyelesaian laporan proposal skripsi ini tidak terlepas dari bantuan pihak terutama kepada Ayah dan Ibu yaitu (alm)Sabar Menanti Panjaitandan Nurhani Manurungyang telah memberikan bantuan moril maupun materil, semangat dan do’a yang begitu besar kepada penulis.

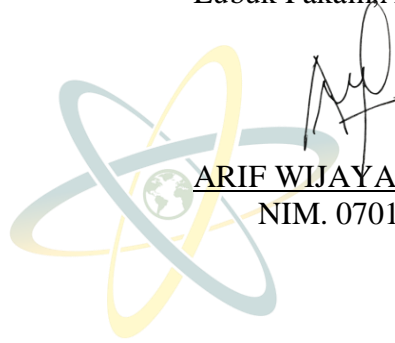
Penulis menyadari bahwa tersusunnya proposal skripsi ini atas do’a, perhatian, bantuan, bimbingan, motivasi serta dukungan dari berbagai pihak, sehingga dengan keikhlasan dan kerendahan hati pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Terima kasih yang sebesar-besarnya kepada kedua orang tua tercinta (ALM) Sabar Menanti Panjaitan dan Nurhani Manurung atas bantuan moril dan materil, semangat dan doa yang besar kepada penulis.

2. Special thanks to all my brother atas obrolannya yang sangat bermanfaat, bantuan moril dan materil, semangat dan doa yang besar untuk penulis setiap hari
3. Prof. Dr. H. Syahrin Harahap, M.A., Rektor Universitas Islam Negeri Sumatera Utara.
4. Bapak Dr. Syahnan, Maryland, MA, Dekan Sekolah Tinggi Sains dan Teknologi Universitas Islam Nasional Sumatera Utara
5. Bapak Ilka zufria, M.Kom selaku ketua Jurusan Ilmu Komputer dan pembimbing skripsi I, membantu penulis dengan ide, saran, kritik dan pengarahan proposal selama penulisan skripsi.
6. Bapak Yusuf Ramadhan Nasution, M.Kom selaku pembimbing skripsi II, membantu penulis dengan ide, saran, kritik dan bimbingan selama penulisan proposal skripsi. Bapak Rakhmat Kurniawan, R., M.Kom selaku Sekretaris Jurusan Ilmu Komputer dan selaku dosen Pembimbing Akademik.
7. Seluruh dosen dan staf Program Studi S1 Ilmu Komputer Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara.
8. Sahabat Persatuan Mahasiswa Deli Serdang (PERMADES) yang telah memberikan arahan dan bertukar pikiran bagi penulis.
9. Teman Forum Pertukaran Belajar Tempat Kerja Mahasiswa (FOKUSMAKER) yang pernah membimbing dan berkomunikasi dengan penulis.
10. Sahabat Komputer 3 yang memberi nasehat, bertukar pikiran dan menemani membaca - Sahabat Komputer, semoga Sahabat Komputer 3 di masa wabah ini tetap aktif melakukan kegiatan dan menyelesaikan perkuliahan akademik secepatnya.
11. Dan semua pihak yang telah membantu penulis menyelesaikan makalah ini. Penulis menyadari bahwa masih terdapat kekurangan dalam makalah ini. Penulis ingin memberikan kritik dan saran yang bersifat membangun demi perbaikan skripsi ini. Tesis ini ditulis untuk memenuhi mata kuliah Program Studi Profesi Ilmu Komputer

UIN SUMATERA UTARA MEDAN. Semoga hasil dan artikel ini bermanfaat bagi pihak yang berkepentingan. **Wassalamu'alaikum Wr. Wb**

Lubuk Pakam, April 2022



ARIF WIJAYA PANJAITAN
NIM. 0701163093



UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

DAFTAR ISI

ABSTRAK.....	i
KATA PENGANTAR.....	ii
DAFTAR ISI.....	iv
DAFTAR GAMBAR.....	vi
DAFTAR TABEL.....	vii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
BAB II TINJAUAN PUSTAKA.....	5
2.1 Keamanan Data Komputer.....	4
2.2 Kriptografi.....	4
2.2.1 Aspek Keamanan Kriptografi.....	5
2.2.2 Serangan Terhadap Kriptografi.....	6
2.2.3 Pengelompokan Algoritma Kriptografi.....	6
2.3 Algoritma Data Encryption Standard.....	9
2.4 File PDF.....	16
2.5 Tabel Ascii.....	17
2.6 PHP.....	17
2.7 Flowchart.....	19
2.8 Penelitian Terkait.....	21

BAB III	METODE PENELITIAN	23
3.1	Tempat dan Waktu Penelitian	23
3.1.1	Tempat Penelitian	24
3.1.2	Waktu & Jadwal Pelaksanaan Penelitian	24
3.2	Metode pengumpulan data	24
3.3	Model Penelitian	24
3.3.1	Perencanaan	25
3.3.2	Analisa kebutuhan	26
3.3.3	Perancangan	26
3.3.4	Implementasi	27
3.3.5	Pengujian	29
3.3.6	Pengunaan	29
BAB IV	HASIL DAN PEMBAHASAN.....	37
4.1	Pembahasan	37
4.1.1	Analisa Data.....	37
4.1.2	Representasi	37
4.1.3	Hasil Analisa Data.....	40
4.1.4	Flowchart Sistem.....	85
4.1.5	Pengujian	87
4.1.6	Implementasi.....	88
4.1.7	Hasil pengujian enkripsi dan deskripsi.....	93
BAB V	KESIMPULAN DAN SARAN.....	94
5.1	Kesimpulan.....	94
5.2	Saran.....	94
DAFTAR PUSTAKA		

DAFTAR GAMBAR

Gambar	Judul Gambar	Halaman
2.1	Diagram enkripsi dan dekripsi kunci simetri	7
2.2	Diagram enkripsi dan dekripsi kunci simetri	8
2.3	Fungsi <i>Hash</i>	9
2.4	Struktur DES	10
2.5	Proses membangkitkan kunci DES	11
2.6	Proses Permutasian DES.....	12
2.7	Proses Round Fuction DES.....	13
2.8	Proses Ekspansi DES.....	13
2.9	Tabel Ekspansi DES	14
2.10	Proses Subtitusi S-BOX DES	14
2.11	Aturan Proses Subtitusi S-BOX.....	14
2.12	Tabel P-BOX DES	16
2.13	Tabel Ascii 0-127.....	17
2.14	Tabel Ascii 28-225	18
3.1	Bagan Langkah Penelitian	26
3.2	Tahap Penelitian.....	27
3.3	Diagram Enkripsi DES	28
3.4	Diagram Deskripsi DES	28
3.5	(a)Flowchart Proses Enkripsidan (b) Dekripsi File PDF.....	29
4.1	File PDF sampel	37
4.2	Nilai pdf sample	38
4.3	Tabel ASCII 0-127	38
4.4	Flowchart enkripsi & deskripsi	85
4.5	Flowchart Antar Muka Masukan	88
4.6	Tampilan Aplikasi	87
4.7	Tampilan Input File Pdf dan Kunci	89
4.8	Tampilan Pdf setelah dienkripsi	89

4.9	Tampilan isi file PDF setelah di enkripsi.....	90
4.10	Tampilan File Pdf menggunakan Dokumen Setelah di enkripsi.....	81
4.11	Tampilan Input PDF dengan kunci yang salah	92
4.12	Tampilan file PDF setelah di enkripsi dengan kunci salah	92
4.13	Tampilan input File PDF dengan kunci benar	93
4.14	Tampilan File PDF setelah dideskripsi dengan kunci benar.....	93



UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

DAFTAR TABEL

Tabel	Judul Tabel	Halaman
2.1	Permuted Choice 1 (PC ⁻¹).....	11
2.2	Permuted Choice 2 (PC ⁻²).....	12
2.3	Initial Permutation (IP)	12
2.4	Inverse Initial Permutation (IP ⁻¹).....	13
2.5	Nilai 8 S-BOX DES.....	15
2.6	Tabel simbol-simbol dan kegunaan simbol-simbol flowchart.....	19
2.7	Tabel Penelitian.....	21
3.1	Waktu dan Jadwal Penelitian	24
3.2	Kebutuhan hardware.....	26
4.1	Biner Data IV Pdf.....	39
4.2	Biner Kunci	39
4.3	Inisial Permutasian	41
4.4	Tabel PC-1	41
4.5	Tabel left shift	42
4.6	Tabel PC-2	45
4.7	Tabel ekspansi	48
4.8	Tabel P-Box	52
4.9	Tabel IP-1.....	75
4.10	Pengujian Sistem	87
4.11	Hasil pengujian Sistem	93

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

DAFTAR LAMPIRAN

Lampiran	Judul lampiran
1. Lampiran I	List Program
2. Lampiran II	Daftar Riwayat Hidup
3. Lampiran III	Kartu Bimbingan Skripsi



UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN