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

**SKRIPSI**



**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 Mencpai Gelar Sarjana komputer*




**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 saudari,

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

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

Medan, 10 Maret 2021

26 Rajab 1442 H



Komisi Pembimbing,

| Pembimbing I, | Pembimbing II, |
|---|---|
| Ilka zufria, M.Kom. | Yusuf Ramadhan Nasution, M.Kom |
| NIP. 198506042015031006 | NIB. 1100000075 |

**SURAT PERNYATAAN KEASLIAN SKIRPSI**

Saya yang bertanda tangan di bawa ini

| | |
|---|---|
| Nama | : ARIF WIJAYA PANJAITAN |
| Nomor Induk Mahasiswa | :070l163093 |
| Program Study | .Ilmu Komputer |
| Judul | :Implementasi Algoritma Data Encryption 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,2l april 2022

ARIF WIJAYA PANJAITAN
NIM.0701163093

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
UIN Sumatera Utara Medan,

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

# 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 Standart, Portable Dokument Format

**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

## KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ 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 materiil, 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

## DAFTAR ISI

## DAFTAR GAMBAR

## DAFTAR TABEL

## DAFTAR LAMPIRAN