

**TUGAS AKHIR**

**PENERAPAN METODE *TRIPLE DATA ENCRYPTION STANDART* (3DES)  
PADA FILE DOC**

Disusun untuk melengkapi dan memenuhi syarat kelulusan program studi strata 1  
Program Studi Teknik Informatika Fakultas Teknik  
Universitas Muhammadiyah Jember



Oleh :

Dirga Rahman Kharisma Burhanudin

1310651122

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS MUHAMMADIYAH JEMBER  
2018**

**HALAMAN PENGESAHAN**

**PENERAPAN METODE *TRIPLE DATA ENCRYPTION STANDART* (3DES)  
PADA FILE *DOC***

**DIRGA RAHMAN KHARISMA BURHANUDIN**

**1310651122**

**Proposal Tugas Akhir ini Diajukan Sebagai Salah Satu Syarat Untuk  
Memperoleh Gelar Sarjana Komputer (S.Kom)**

di

Universitas Muhammadiyah Jember

Disetujui Oleh :

Dosen Pembimbing I

Dosen Pembimbing II

**Victor Wahanggara, S.kom, M.kom**  
NPK. 12 03 375

**Henny Wahyu Sulisty, S.kom,  
M.kom**  
NPK. 10 09 550

Dosen Penguji I

Dosen Penguji II

**Ginajar Abdurrahman, S.Si, M.Pd**  
NPK. 15 09 637

**Daryanto, S.Kom, M.Kom**  
NPK. 11 03 589

Mengesahkan,  
Dekan Fakultas Teknik

Mengetahui,  
Ketua Program Studi Teknik Informatika

**Ir. Suhartinah, M.T.**  
NPK. 95 05 246

**Yeni Dwi Rahayu, S.ST, M.Kom.**  
NPK. 11 03 59

## **PERNYATAAN**

Yang bertandatangan di bawah ini :

NIM : 13 1065 1122

Nama : Dirga Rahman Kharisma Burhanudin

Institusi : Program Studi Teknik Informatika, Fakultas Teknik, Universitas  
Muhammadiyah Jember

Menyatakan bahwa Tugas Akhir yang berjudul **“PENERAPAN METODE TRIPLE DATA ENCRYPTION STANDART PADA FILE DOC”**. Bukan merupakan karya orang lain kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini dibuat dengan sebenar-benarnya dan apabila pernyataan ini tidak benar penulis bersedia mendapatkan sanksi dari akademik.

Jember, 27 Maret 2018

**Dirga Rahman Kharisma B**  
**NIM. 13 1065 1122**

## **PENERAPAN METODE *TRIPLE DATA ENCRYPTION STANDART (3DES)* PADA FILE DOC**

<sup>1</sup>Dirga Rahman Kharisma Burhanudin 1310651122

<sup>2</sup>Victor Wahanggara, S.kom, M.kom, <sup>3</sup>Henny Wahyu Sulisty S.Kom, M.Kom

Jurusan Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember

Jln. Karimata No 49, Telp (0331)336728, jember

[devildice999@gmail.com](mailto:devildice999@gmail.com)

### **ABSTRAK**

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi, terutama yang berisi informasi sensitif yang hanya diketahui isinya oleh pihak tertentu, sehingga perlu dilakukan penyandian data supaya berapa pihak yang tidak memiliki kewenangan tidak akan dapat membuka informasi yang dikirim. Di Universitas Muhammadiyah Jember menjelaskan bahwa ilmu yang mempelajari tentang proses pengamanan data adalah kriptografi. *Triple DES* adalah sebuah *chipper* blok yang dibentuk oleh DES dengan menggunakan DES tiga kali. Penggunaan tiga langkah ini penting untuk mencegah *meet – in – middle attack* sebagai mana pada *Double DES*. Dari hasil enkripsi file dokumen dengan metode 3DES dilakukan 10 kali percobaan menggunakan file dokumen yang berbeda, berhasil dilakukan dan tidak ada error yang terjadi saat proses enkripsi dan dekripsi.

**Kata kunci : kriptografi, enkripsi, dekripsi 3DES**

**PENERAPAN METODE *TRIPLE DATA ENCRYPTION STANDART* (3DES)  
PADA FILE DOC**

<sup>1</sup>Dirga Rahman Kharisma Burhanudin 1310651122

<sup>2</sup>Victor Wahanggara, S.kom, M.kom, <sup>3</sup>Henny Wahyu Sulisty S.Kom, M.Kom

Jurusan Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember

Jln. Karimata No 49, Telp (0331)336728, jember

[devildice999@gmail.com](mailto:devildice999@gmail.com)

**ABSTRACT**

*Data security is very important in maintaining the confidentiality of information, especially those containing sensitive information that is only known contents by certain parties, so it is necessary to do data encryption so that unauthorized parties will not be able to disclose the information sent. At the University of Muhammadiyah Jember explained that the science that studies about the process of securing data is cryptography. Triple DES is a chip blocker formed by DES by using DES three times. The use of these three steps is important to prevent the meet - in - middle attack as in Double DES. From the result of encrypting document file with 3DES method done 10 times experiment using different document file, successfully done and no error happened during process of encryption and decryption.*

**Keywords: *cryptography, encryption, decryption 3DES***

## HALAMAN PERSEMBAHAN



Dengan hormat saya ucapkan banyak terima kasih dan karya ini dipersembahkan kepada :

1. Allah SWT, dengan niat menuntut ilmu untuk beribadah dan memohon Ridho Mu Ya Rabb.
2. Orang tua tercinta, yang selalu memberikan doa, dukungan dan motivasi dalam mengerjakan Tugas Akhir ini.
3. Bapak Victor Wahanggara, S.Kom, M.Kom dan Bapak Henny Wahyu Sulistyio S.Kom, M.Kom selaku pembimbing serta seseorang yang selalu memotivasi saya dalam belajar.
4. Bapak Daryanto, S.Kom M.Kom dan Ginanjar Abdurrahman, S.Si M.Pd, selaku penguji 1 dan 2 yang telah membantu menyempurnakan Tugas Akhir.
5. Teman-Teman ngopi saat mencari inspirasi Ahmad Supriyadi Raharjo, Saifur rizal, Nanang Sugiarto, Hilman Nurharis, Rizal Pranata dan masih banyak lagi yang tidak bisa saya sebutkan satu persatu.
6. Teman-Teman penyemangat mas ahong, mas sodek, ajis, dll.
7. Dan seluruh pihak yang tidak bisa saya sebutkan satu per satu.

## UNGKAPAN TERIMA KASIH



Alhamdulillah Segala puji bagi Allah SWT Rabb semesta alam, berkat rahmat dan kasih sayang-Nya sehingga saya dapat menyelesaikan Tugas Akhir ini. Sholawat serta salam selalu tercurah kepada tauladan sepanjang masa, Nabi Muhammad shallallahu alaihi wasallam, beserta para keluarga, sahabat, dan para pengikutnya yang senantiasa istiqomah dalam sunnahnya hingga akhir jaman.

Penulis menyadari sepenuhnya bahwa begitu banyak pihak yang telah turut membantu dalam penyelesaian skripsi ini. Melalui kesempatan ini, dengan segala kerendahan hati, penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Ibu Ir. Suhartinah, M.T. selaku dekan Fakultas Teknik Universitas Muhammadiyah Jember.
2. Ibu Yeni Dwi Rahayu S. ST., M.Kom selaku ketua prodi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember.
3. Bapak Victor Wahanggara, S.Kom, M.Kom dan Bapak Henny Wahyu Sulisty S.Kom, M.Kom selaku pembimbing 1 dan pembimbing 2.
4. Bapak Ginanjar Abdurrahman, S.Si M.Pd dan Daryanto, S.Kom M.Kom selaku dosen penguji 1 dan dosen penguji 2.
5. Semua dosen Program Studi Informatika, terima kasih atas semua ilmu yang telah diberikan.
6. Semua teman-teman yang telah membantu, membagi ilmu serta pengalamannya kepada saya, semoga Allah membalas kebaikan kalian semua dan mengangkat derajat mereka orang yang berilmu.
7. Dan seluruh pihak yang tidak bisa saya sebutkan satu per satu.

## MOTO

*Berpikir sebelum bertindak itu penting*

*Tetapi jangan terlalu lama berpikir*

*Salah satu kegagalan adalah*

*Terlalu lama berpikir*

*(Dirga Rahman)*



## KATA PENGANTAR



Puji dan syukur penulis panjatkan kehadiran Allah SWT yang telah melimpahkan kasih dan sayang-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul :

### **PENERAPAN METODE *TRIPLE DATA ENCRYPTION STANDART* (3DES) PADA FILE DOC**

Sholawat serta salam selalu tercurah kepada tauladan sepanjang masa, Nabi Muhammad shallallahu alaihi wasallam, beserta para keluarga, sahabat, dan para pengikutnya yang senantiasa istiqomah dalam sunnahnya hingga akhir jaman.

Maksud dari penyusunan Tugas Akhir ini adalah untuk mengetahui cara penyandian menggunakan kriptografi dengan metode 3DES pada file dokumen.

Dengan kerendahan hati, penulis memohon maaf secara pribadi jika di kemudian hari terdapat ketidaksempurnaan terhadap pengerjaan Tugas Akhir. Dan semoga penulisan Tugas Akhir ini bisa bermanfaat bagi pengembang ilmu atau setiap insan yang selalu belajar dan menuntut ilmu.

Jember, 27 maret 2018

Penulis

## DAFTAR ISI

<b>HALAMAN SAMPUL</b> .....	i
<b>HALAMAN PENGESAHAN</b> .....	ii
<b>PERNYATAAN</b> .....	iii
<b>DAFTAR ISI</b> .....	iv
<b>DAFTAR GAMBAR</b> .....	vi
<b>DAFTAR TABEL</b> .....	vii
<b>BAB I PENDAHULUAN</b> .....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan Penelitian .....	2
1.4 Batasan Masalah .....	2
1.5 Manfaat Penelitian .....	2
<b>BAB II LANDASAN TEORI</b> .....	3
2.1 Penelitian Terdahulu .....	3
2.2 Kriptografi .....	4
2.3 <i>Data Encryption Standard (DES)</i> .....	6
2.3.1 Panjang kunci dan ukuran blok DES.....	7
2.3.2 Teknik dasar Kriptografi.....	8
2.4 <i>Triple Data Encryption Standard (3DES)</i> .....	9
2.4.1 Algoritma 3DES.....	10
2.4.1.1 Proses Enkripsi 3DES .....	12
2.4.1.2 Proses Dekripsi 3DES.....	12
2.4.2 Keamanan 3DES .....	12
2.4.3 Implementasi Kriptografi.....	13
2.5 Visual Studio VB.NET.....	13

<b>BAB III METODOLOGI PENELITIAN .....</b>	<b>17</b>
3.1 Studi Literatur.....	18
3.2 Analisa kebutuhan.....	18
3.2.1 Analisa kebutuhan perangkat keras.....	18
3.2.2 Analisa kebutuhan perangkat lunak .....	19
3.3 Skema dan Desain .....	20
3.3.1 Desain <i>interface</i> aplikasi 3DES .....	20
3.4 Implementasi .....	21
3.5 Pengujian .....	21
3.6 Hasil analisa.....	21
3.7 Pembahasan metode 3DES.....	21
3.7.1 Proses enkripsi 3DES .....	22
<b>BAB IV HASIL DAN PEMBAHASAN.....</b>	<b>35</b>
4.1 Implementasi.....	35
4.2 Pengujian Program.....	35
<b>BAB V KESIMPULAN DAN SARAN .....</b>	<b>39</b>
5.1 Kesimpulan.....	39
5.2 Saran.....	39
<b>DAFTAR PUSTAKA .....</b>	<b>40</b>
<b>LAMPIRAN .....</b>	<b>41</b>

## DAFTAR GAMBAR

Gambar 1 Diagram proses enkripsi dan dekripsi.....	6
Gambar 2 Skema Global Algoritma DES .....	7
Gambar 4 Enkripsi dengan permutasi.....	9
Gambar 5 Enkripsi dengan Ekspansi .....	9
Gambar 6 Diagram enkripsi dan dekripsi 3DES .....	10
Gambar 7 Tahapan algoritma .....	11
Gambar 8 Antarmuka <i>Visual Studio</i> .....	14
Gambar 9 <i>Toolbox</i> .....	15
Gambar 10 Tahapan Penelitian .....	17
Gambar 11 Algoritma 3DES .....	20
Gambar 12 Rancangan dari tampilan <i>interfaces</i> .....	20
Gambar 13 Enkripsi EEE 3DES .....	21
Gambar 14 Dekripsi EEE 3DES.....	22
Gambar 15 Enkripsi EDE 3 DES .....	22
Gambar 16 Dekripsi EDE 3 DES .....	22
Gambar 17 Program utama .....	35
Gambar 18 Lokasi file yang di enkripsi.....	36
Gambar 19 Pesan sukses di enkripsi.....	36
Gambar 20 Proses dekripsi.....	37
Gambar 21 Pesan sukses di dekripsi.....	37
Gambar 22 Hasil file enkripsi.....	38

## DAFTAR TABEL

Tabel 1 Spesifikasi Laptop.....	18
Tabel 2 Inisial Permutasi (IP).....	23
Tabel 3 PC-1.....	24
Tabel 4 Tabel <i>Left Shift</i> .....	25
Tabel 5 PC-2.....	26
Tabel 6 Ekspansi (E).....	27
Tabel 7 S-BOX 1 .....	28
Tabel 8 S-BOX 2 .....	28
Tabel 9 S-BOX 3 .....	28
Tabel 10 S-BOX 4 .....	28
Tabel 11 S-BOX 5 .....	29
Tabel 12 S-BOX 6 .....	29
Tabel 13 S-BOX 7 .....	29
Tabel 14 S-BOX 8 .....	29
Tabel 15 S-BOX 1 biner .....	30
Tabel 16 P-BOX.....	31
Tabel 17 IP <sup>-1</sup> .....	33
Tabel 18 Hasil enkripsi dan dekripsi .....	38