

ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD*

(AES) 256 PADA APLIKASI TABUNGAN SANTRI

BERBASIS WEB



SKRIPSI

Diajukan Kepada Fakultas Matematika dan Ilmu Komputer UNUGHA Cilacap

guna memperoleh gelar Kesarjanaan Strata 1 dalam bidang

Matematika dan Ilmu Komputer

Oleh

MUHAMAD HASANUDIN

NIM 17552011010

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU KOMPUTER

UNIVERSITAS NAHDLATUL ULAMA AL GHAZALI CILACAP

2022

PENGESAHAN

Skripsi Saudara
Nama : Muhamad Hasanudin
NIM : 17552011010
Fakultas/Prodi : Fakultas MIKOM / Teknik Informatika
Judul : Algoritma Kriptografi *Advanced Encryption Standard (AES) 256* pada Aplikasi Tabungan Santri

Telah disidangkan oleh Dewan Penguji Fakultas Matematika dan Ilmu Komputer Universitas Nahdlatul Ulama Al Ghazali (UNUGHA) Cilacap pada hari / tanggal :

Senin, 31 Januari 2022

Dan dapat diterima sebagai pemenuhan tugas akhir mahasiswa Program Strata 1 (S.1) Teknik Informatika (TI) Fakultas Matematika dan Ilmu Komputer (FMKOM) pada Universitas Nahdlatul Ulama Al Ghazali (UNUGHA) Cilacap.

Cilacap, 31 Januari 2022

Dewan Sidang

Ketua

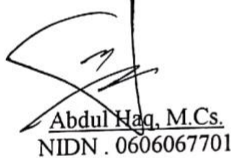

H. Edy Sulistiyanto, SH., M.Kom.
NIDN. 0613065801

Sekretaris



Safiq Rosad, M.Kom
NIDN. 0609018101

Penguji 1


Abdul Haq, M.Cs.
NIDN . 0606067701

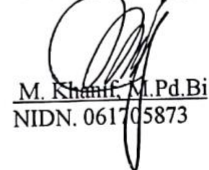
Penguji 2


Safiq Rosad, M.Kom.
NIDN. 0609018101

Pembimbing


Lasimin, M.Kom.
NIDN. 0605048602

Ass. Pembimbing


M. Khair, M.Pd.Bi
NIDN. 061705873

Dekan Fakultas Matematika dan Ilmu Komputer
Universitas Nahdlatul Ulama Al Ghazali Cilacap



H. Edy Sulistiyanto, S.H., M.Kom.
NIDN. 0613065801

NOTA KONSULTAN

Dosen Fakultas Matematika dan Ilmu Komputer Universitas Nahdlatul Ulama Al
Ghazali (UNUGHA) Cilacap

Hal : Skripsi Saudara Muhamad Hasanudin
Lampiran : -

Kepada:
Yth. Bapak Dekan FMIKOM
UNUGHA Cilacap
di-
Cilacap

Assalamu'alaikum Wr. Wb.

Setelah saya membaca, memeriksa dan mengadakan perbaikan seperlunya,
maka konsultan berpendapat bahwa skripsi saudara :

Nama : Muhamad Hasanudin
NIM : 17552011010
Judul : Algoritma Kriptografi *Advanced Encryption
Standard (AES) 256* pada Aplikasi Tabungan Santri

Telah dapat diajukan kepada Fakultas Matematika dan Ilmu Komputer
(FMIKOM) pada Universitas Nahdlatul Ulama Al Ghazali (UNUGHA) Cilacap
untuk memenuhi syarat memperoleh gelar Stara Satu (S1).

Wassalamu'alaikum Wr. Wb.

Cilacap, 21 Februari 2022
Konsultan


ABDUL NAO M.Cs
0606067701

NOTA PEMBIMBING

Cilacap, 4 Januari 2022

Kepada Yth :
Kaprodik Teknik Informatika
Fakultas Matematika Dan Komputer (FMKOM)
UNUGHA Cilacap
Di Tempat

Assalamu'alaikum Wr. Wb.

Setelah melakukan bimbingan, telaah, arahan dan koreksi tahap penulisan skripsi saudara:

Nama : Muhamad Hasanudin
NIM : 17552011010
Fakultas : Matematika dan Ilmu Komputer (MIKOM)
Prodi : Teknik Informatika
Judul : Algoritma Kriptografi *Advanced Encryption Standard*
(AES) 256 Pada Aplikasi Tabungan Santri

Kami berpendapat bahwa skripsi tersebut sudah dapat diajukan ke sidang munaqosah.

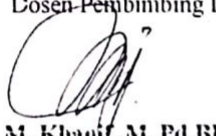
Bersamaan ini kami kirimkan skripsi tersebut, semoga dapat segera dimunaqasahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum Wr. Wb.

Mengetahui,

Dosen Pembimbing I

Lasimin, M.Kom
0605048602

Dosen Pembimbing II

M. Khanif, M. Pd.Bi
0617058703

PERNYATAAN KEORISINILAN

Yang bertanda tangan dibawah ini:

Nama : Muhamad Hasanudin
NIM : 17552011010
Fakultas : Matematika dan Ilmu Komputer (MIKOM)
Prodi : Teknik Informatika
Judul : Algoritma Kriptografi *Advanced Encryption Standard*
(AES) 256 Pada Aplikasi Tabungan Santri

Menyatakan bahwa skripsi ini benar-benar orisinal atau buatan sendiri, tidak ada unsur menjiplak atau dibuatkan. Jika dikemudian hari ditemukan adanya indikasi salah satu dari unsur diatas, maka saya bersedia dicabut gelar keserjanaanya.

Demikian surat pernyataan ini dibuat dengan penuh kesadaran dan tanpa ada unsur paksaan.

Cilacap, 15 Februari 2022
Yang menyatakan



Muhamad Hasanudin
NIM.17552011010

HALAMAN MOTTO

وَإِذْ تَأْتِيَنَّكُمْ رَبُّكُمْ لِئِنْ شَكَرْتُمْ لَأَزِيدَنَّكُمْ وَلَئِنْ كَفَرْتُمْ إِنَّ عَذَابِي لَشَدِيدٌ

Dan (ingatlah juga), tatkala Tuhanmu memaklumkan; "Sesungguhnya jika kamu bersyukur, pasti Kami akan menambah (nikmat) kepadamu, dan jika kamu mengingkari (nikmat-Ku), maka sesungguhnya azab-Ku sangat pedih"
(QS Ibrahim Ayat 7)

إِنَّمَا الْأَعْمَالُ بِالنِّيَّةِ وَإِنَّمَا لِكُلِّ مَن نَّوَى

“Sesungguhnya segala perbuatan itu bergantung pada niatnya, dan setiap orang akan mendapatkan apa yang diniatkannya” (HR. Bukhari Muslim)

“Don’t judge a book by it's cover”

jangan menilai seseorang hanya dengan melihat penampilannya apalagi bila belum mengenalnya.

HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT, Rabb semesta alam yang senantiasa memberikan karunia sehingga penulis mampu menyelesaikan penulisan skripsi ini.

Karya ini saya persembahkan kepada:

1. Orang tua (Bapak Muhamad Nurohman dan Ibu Umi Choeriyah) Sebagai tanda bakti, hormat dan rasa terima kasih yang tiada terhingga yang telah selalu memdidik, memberikan do'a, dukungan, nasihat dan semangat yang tiada henti.
2. Saudaraku tercinta (Khusni Laelatun Ni'mah dan Mohamad Ngazizun Hakim) yang selalu memberikan doa dan semangat tiada henti.
3. Keluarga FMIKOM 2017 yang selalu memberikan keceriaan, kebersamaan dan motivasi.
4. Seluruh teman UNUGHA yang telah memberikan do'a, dukungan, dan semangat.

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Alhamdulillahillobbi ‘alamin, puji syukur dipanjatkan ke hadirat Allah SWT yang telah melimpahkan rahmat, taufiq dan KaruniaNya sehingga penulis dapat menyelesaikan skripsi ini dengan judul “**Algoritma Kriptografi *Advanced Encryption Standard (AES) 256* pada Aplikasi Tabungan Santri**”, sebagai salah satu syarat untuk menyelesaikan program Sarjana (S1) jurusan Teknik Informatika Fakultas Matematika dan Ilmu Komputer UNUGHA.

Penulis menyadari bahwa skripsi ini tidak mungkin terselesaikan tanpa adanya dukungan, bantuan, bimbingan dan nasihat dari berbagai pihak selama penyusunan skripsi ini. Pada kesempatan kali ini penulis menyampaikan terima kasih setulus - tulusnya kepada:

1. Direktorat Jenderal Pendidikan Tinggi, Riset dan Teknologi, Kemendikbudristek yang telah memberikan kesempatan dan dukungan secara materiil.
2. Rektor Universitas Nahdlatul Ulama Al-Ghazali (UNUGHA) Cilacap, Bapak Drs. K.H. Nasrulloh, M.H.
3. Dekan Fakultas Matematika dan Ilmu Komputer (FMIKOM) Universitas Nahdlatul Ulama Al-Ghazali (UNUGHA) Cilacap, Bapak H. Edy Sulistiyanto, S.H., M.Kom.
4. Bapak Lasimin, M.Kom. selaku pembimbing I yang juga telah meluangkan waktu untuk memberikan bimbingan dan masukan dalam menyelesaikan skripsi ini.
5. Bapak Lasimin, M.Kom. selaku pembimbing I yang juga telah meluangkan waktu untuk memberikan bimbingan dan masukan dalam menyelesaikan skripsi ini.
6. Bapak Muhammad Khanif M. Pd.BI selaku pembimbing II yang telah meluangkan waktu untuk memberikan bimbingan dan arahan dalam menyelesaikan skripsi ini.
7. Seluruh Dosen yang pernah mengajar dan membimbing penulis selama kuliah

di Program Studi Teknik Informatika, Fakultas Matematika Ilmu dan Komputer Universitas Nahdlatul Ulama Al-Ghazali (UNUGHA) Cilacap.

8. Kyai Mukhammad Lutfillah selaku Pengasuh Pondok Pesantren Asaasunnajaah Kesugihan yang telah memberikan izin pelaksanaan penelitian skripsi ini.
9. Teman-teman mahasiswa FMIKOM 2017 yang telah kebersamai penulis selama empat tahun di bangku perkuliahan.
10. Orang tua tercinta, saudara, keponakan dari keluarga besar yang selalu mendoakan, memberikan dukungan, dan semangat penulis untuk selalu berjuang dalam menyelesaikan skripsi.
11. Keluarga besar Pondok Pesantren Asaasunnajaah Kesugihan yang selalu menjadi menginspirasi penulis untuk tetap berjuang dalam menyelesaikan skripsi.
12. Semua pihak, secara langsung maupun tidak langsung yang tidak dapat saya sebutkan satu per satu.

Dalam penulisan skripsi ini masih banyak kekurangan dan kesalahan, karena itu segala kritik dan saran yang membangun akan menyempurnakan penulisan skripsi ini serta bermanfaat bagi penulis dan pembaca.

Cilacap, 15 Februari 2022

Penulis,

Muhamad Hasanudin
NIM.17552011010

DAFTAR ISI

PENGESAHAN	II
NOTA KONSULTAN	III
NOTA PEMBIMBING	IV
PERNYATAAN KEORISINILAN	V
HALAMAN MOTTO	VI
HALAMAN PERSEMBAHAN	VII
DAFTAR ISI	X
DAFTAR GAMBAR	XIII
DAFTAR TABEL	XV
BAB I	1
PENDAHULUAN	1
A. LATAR BELAKANG	1
B. RUMUSAN MASALAH	3
C. TUJUAN PENELITIAN	3
D. BATASAN PENELITIAN	3
E. MANFAAT PENELITIAN	4
F. SISTEMATIKA PENULISAN	5
BAB II	6
KAJIAN PUSTAKA	6
A. KAJIAN PUSTAKA	6
B. LANDASAN TEORI	8
1. Kriptografi	8
2. Advanced Encryption Standard (AES)	10
3. Aplikasi Berbasis Web	14
4. Keamanan Sistem Perbankan	17

BAB III.....	18
METODOLOGI PENELITIAN	18
A. METODOLOGI PENELITIAN	18
1. Observasi dan Penggalian Data	19
2. Analisis Kebutuhan Sistem.....	19
3. Desain UI dan Database.....	21
B. METODE PENGEMBANGAN SISTEM	46
C. METODE KEAMANAN SISTEM	47
D. JADWAL PENELITIAN.....	48
BAB IV	49
IMPLEMENTASI DAN PEMBAHASAN.....	49
A. IMPLEMENTASI SISTEM.....	49
1. Halaman Login	49
2. Halaman Dashboard	50
3. Halaman List Admin.....	50
4. Halaman Input Admin.....	51
5. Halaman List Nasabah.....	51
6. Halaman Input Nasabah.....	52
7. Halaman List Penyetoran	52
8. Halaman Input Penyetoran	53
9. Halaman List Penarikan.....	53
10. Halaman Input Penarikan	54
B. IMPLEMENTASI ALGORITMA AES-256.....	54
C. PENGUJIAN	58
1. Pengujian Keamanan Database Server	58
2. Pengujian Brute Force	59
D. MAINTENANCE	63
BAB V.....	64
PENUTUP.....	64

A. KESIMPULAN.....	64
B. SARAN.....	64
DAFTAR PUSTAKA	65
LAMPIRAN.....	67

DAFTAR GAMBAR

Gambar 2. 1 Ilustrasi Proses Enkripsi AES	11
Gambar 2. 2 Tabel S-Box <i>SubBytes</i>	12
Gambar 2. 3 Pengaruh Pemetaan pada Setiap <i>Byte</i> dalam <i>State</i>	12
Gambar 2. 4 Transformasi <i>ShiftRows</i>	13
Gambar 3. 1 <i>Flowchart</i> Metodologi Penelitian	18
Gambar 3. 2 Komponen – Komponen <i>Use Case Diagram</i>	23
Gambar 3. 3 <i>Use Case Diagram</i> Aplikasi Tabungan Santri	24
Gambar 3. 4 Symbol Relationships antar class	30
Gambar 3. 5 Angka Kardinalitas.....	30
Gambar 3. 6 Class Diagram Aplikasi Tabungan Santri	31
Gambar 3. 7 <i>Sequence Diagram Login</i>	33
Gambar 3. 8 <i>Sequence Diagram</i> Input Data Santri.....	34
Gambar 3. 9 <i>Sequence Diagram</i> Cek Profil Santri	35
Gambar 3. 10 <i>Sequence Diagram</i> Setor Uang	36
Gambar 3. 11 <i>Sequence Diagram</i> Tarik Uang	37
Gambar 3. 12 <i>User Interface Login</i>	38
Gambar 3. 13 <i>User Interface Dashboard</i>	39
Gambar 3. 14 <i>User Interface</i> List Admin	39
Gambar 3. 15 <i>User Interface</i> Tambah Admin	40
Gambar 3. 16 <i>User Interface</i> List Nasabah.....	40
Gambar 3. 17 <i>User Interface</i> Tambah Nasabah.....	41
Gambar 3. 18 <i>User Interface</i> List Penyetoran	41
Gambar 3. 19 <i>User Interface</i> Tambah Penyetoran.....	42
Gambar 3. 20 <i>User Interface</i> List Penarikan	43
Gambar 3. 21 <i>User Interface</i> Tambah Penarikan.....	43
Gambar 3. 22 Metode Agile SDLC	46
Gambar 4. 1 Halaman <i>Login</i>	49
Gambar 4. 2 Halaman Dashboard	50
Gambar 4. 3 Halaman List Admin	50

Gambar 4. 4 Halaman Input Admin	51
Gambar 4. 5 Halaman List Nasabah	51
Gambar 4. 6 Halaman Input Nasabah	52
Gambar 4. 7 Halaman List Penyetoran	52
Gambar 4. 8 Halaman Input Penyetoran	53
Gambar 4. 9 Halaman List Penarikan	53
Gambar 4. 10 Halaman Input Penarikan	54
Gambar 4. 11 Tampilan <i>Database</i> yang belum terenkripsi	55
Gambar 4. 12 Tampilan tabel admin yang terenkripsi	57
Gambar 4. 13 Tampilan tabel nasabah yang terenkripsi	57
Gambar 4. 14 Tampilan tabel penyetoran yang terenkripsi	57
Gambar 4. 15 Tampilan table penarikan yang terenkripsi	57
Gambar 4. 16 Proses <i>sql injection</i> dengan <i>sqlmap</i> dan hasilnya	58
Gambar 4. 17 Enkripsi menggunakan MD5 Hash Generator	59
Gambar 4. 18 Enkripsi menggunakan SHA256.....	60
Gambar 4. 19 Halaman Web <i>Crack Station</i>	60
Gambar 4. 20 Hasil <i>crack</i> MD5	61
Gambar 4. 21 Hasil <i>crack</i> SHA256	61
Gambar 4. 22 Hasil <i>crack</i> AES-256.....	62

DAFTAR TABEL

Tabel 3. 1 Skenario <i>Use Case</i> Login.....	25
Tabel 3. 2 Skenario Input Data Santri	26
Tabel 3. 3 Skenario Cek Profil Santri	26
Tabel 3. 4 Skenario Setor Uang	27
Tabel 3. 5 Skenario Tarik Uang	28
Tabel 3. 6 Tabel Admin	44
Tabel 3. 7 Tabel Nasabah.....	44
Tabel 3. 8 Tabel Role	44
Tabel 3. 9 Tabel Penyetoran.....	45
Tabel 3. 10 Tabel Penarikan.....	45
Tabel 3. 11 Jadwal Penelitian	48