

## DAFTAR ISI

PERNYATAAN.....	<b>Error! Bookmark not defined.</b>
KATA PENGANTAR.....	<b>Error! Bookmark not defined.</b>
UCAPAN TERIMA KASIH .....	<b>Error! Bookmark not defined.</b>
ABSTRAK .....	<b>Error! Bookmark not defined.</b>
ABSTRACT .....	<b>Error! Bookmark not defined.</b>
DAFTAR ISI .....	vii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR .....	xiii
BAB I .....	<b>Error! Bookmark not defined.</b>
PENDAHULUAN .....	<b>Error! Bookmark not defined.</b>
1.1 Latar Belakang.....	<b>Error! Bookmark not defined.</b>
1.2 Rumusan Masalah .....	<b>Error! Bookmark not defined.</b>
1.3 Batasan Masalah.....	<b>Error! Bookmark not defined.</b>
1.4 Tujuan Penelitian.....	<b>Error! Bookmark not defined.</b>
1.5 Sistematika Penulisan.....	<b>Error! Bookmark not defined.</b>
BAB II.....	<b>Error! Bookmark not defined.</b>
TINJAUAN PUSTAKA .....	<b>Error! Bookmark not defined.</b>
2.1 Implementasi .....	<b>Error! Bookmark not defined.</b>
2.2 Keamanan .....	<b>Error! Bookmark not defined.</b>
2.3 Keamanan Informasi .....	<b>Error! Bookmark not defined.</b>
2.3.1 Tiga Aspek Keamanan Komputer....	<b>Error! Bookmark not defined.</b>
2.4 Otentikasi.....	<b>Error! Bookmark not defined.</b>

2.4.1	Faktor-Faktor Otentikasi .....	<b>Error! Bookmark not defined.</b>
2.4.2	<i>Two-Factor Authentication</i> .....	<b>Error! Bookmark not defined.</b>
2.5	Kriptografi .....	<b>Error! Bookmark not defined.</b>
2.5.1	Tujuan Kriptografi .....	<b>Error! Bookmark not defined.</b>
2.5.2	Karakteristik Kriptografi .....	<b>Error! Bookmark not defined.</b>
2.5.3	Teknik Dasar Kriptografi .....	<b>Error! Bookmark not defined.</b>
2.5.4	Prinsip Shannon .....	<b>Error! Bookmark not defined.</b>
2.6	<i>One-time Password (OTP)</i> .....	<b>Error! Bookmark not defined.</b>
2.6.1	Jenis-jenis <i>One-time Password (OTP)</i> .....	<b>Error! Bookmark not defined.</b>
2.6.2	Cara Kerja <i>One-time Password (OTP)</i> .....	<b>Error! Bookmark not defined.</b>
2.7	<i>Advance Encryption Standard (AES)</i> .....	<b>Error! Bookmark not defined.</b>
2.7.1	Sejarah Algoritma AES .....	<b>Error! Bookmark not defined.</b>
2.7.2	Algoritma AES .....	<b>Error! Bookmark not defined.</b>
2.7.3	Fungsi Transformasi dalam AES .....	<b>Error! Bookmark not defined.</b>
2.7.4	Ekspansi Kunci .....	<b>Error! Bookmark not defined.</b>
2.7.5	Contoh Enkripsi Algoritma AES .....	<b>Error! Bookmark not defined.</b>
2.8	<i>Avalanche Effect</i> .....	<b>Error! Bookmark not defined.</b>
2.9	<i>Hamming Weight</i> .....	<b>Error! Bookmark not defined.</b>
2.10	<i>Randomness Test</i> .....	<b>Error! Bookmark not defined.</b>
2.10.1	Lima Uji Dasar untuk Keacakan .....	<b>Error! Bookmark not defined.</b>
2.11	<i>SMS Gateway dan SMS API</i> .....	<b>Error! Bookmark not defined.</b>
2.11.1	<i>SMS Gateway</i> .....	<b>Error! Bookmark not defined.</b>
2.12	Penelitian Terdahulu .....	<b>Error! Bookmark not defined.</b>
BAB III .....		<b>Error! Bookmark not defined.</b>
METODOLOGI PENELITIAN .....		<b>Error! Bookmark not defined.</b>
3.1	Desain Penelitian .....	<b>Error! Bookmark not defined.</b>

3.2	Metode Penelitian.....	<b>Error! Bookmark not defined.</b>
3.2.1	Metode Pengumpulan Data.....	<b>Error! Bookmark not defined.</b>
3.2.2	Metode Pengembangan Perangkat Lunak.....	<b>Error! Bookmark not defined.</b>
3.3	Alat dan Bahan Penelitian .....	<b>Error! Bookmark not defined.</b>
3.3.1	Alat Penelitian.....	<b>Error! Bookmark not defined.</b>
3.3.2	Bahan Penelitian.....	<b>Error! Bookmark not defined.</b>
BAB IV .....		<b>Error! Bookmark not defined.</b>
HASIL PENELITIAN DAN PEMBAHASAN.....		<b>Error! Bookmark not defined.</b>
4.1	Hasil Penelitian.....	<b>Error! Bookmark not defined.</b>
4.2	Memodifikasi algoritma AES 256 <i>bits</i> dengan S-Box dan ShiftRow yang bergantung pada kunci .....	<b>Error! Bookmark not defined.</b>
4.2.1	S-Box yang Bergantung pada Kunci.....	<b>Error! Bookmark not defined.</b>
4.2.2	ShiftRow yang Bergantung pada Kunci.....	<b>Error! Bookmark not defined.</b>
4.2.3	AES 256 <i>bits</i> .....	<b>Error! Bookmark not defined.</b>
4.3	Membangkitkan Kode Otentikasi.....	<b>Error! Bookmark not defined.</b>
4.3.1	Alur Membangkitkan dan Memecahkan Kode Otentikasi.....	<b>Error! Bookmark not defined.</b>
4.4	Proses Pengiriman Kode Otentikasi .....	<b>Error! Bookmark not defined.</b>
4.5	Pengembangan Perangkat Lunak .....	<b>Error! Bookmark not defined.</b>
4.5.1	Deskripsi Sistem .....	<b>Error! Bookmark not defined.</b>
4.5.2	Batasan Perangkat Lunak.....	<b>Error! Bookmark not defined.</b>
4.5.3	Proses Operasional Perangkat Lunak.....	<b>Error! Bookmark not defined.</b>
4.5.4	Perancangan .....	<b>Error! Bookmark not defined.</b>
4.5.5	Implementasi .....	<b>Error! Bookmark not defined.</b>
4.5.6	Pengujian.....	<b>Error! Bookmark not defined.</b>
4.6	Pembahasan Modifikasi AES 256 bits ....	<b>Error! Bookmark not defined.</b>

4.6.1	Perbandingan dan Pengujian AES 256 <i>bits</i> standard dan yang telah dimodifikasi .....	<b>Error! Bookmark not defined.</b>
4.6.2	Analisis Hasil Uji Modifikasi AES 256 <i>bits</i> ..	<b>Error! Bookmark not defined.</b>
BAB V.....		<b>Error! Bookmark not defined.</b>
KESIMPULAN DAN SARAN.....		<b>Error! Bookmark not defined.</b>
5.1	Kesimpulan.....	<b>Error! Bookmark not defined.</b>
5.2	Saran.....	<b>Error! Bookmark not defined.</b>
DAFTAR PUSTAKA .....		<b>Error! Bookmark not defined.</b>
LAMPIRAN.....		<b>Error! Bookmark not defined.</b>
Lampiran 1. Contoh proses Enkripsi Algoritma Modifikasi AES 256 <i>bits</i> .		<b>Error! Bookmark not defined.</b>
RIWAYAT HIDUP .....		<b>Error! Bookmark not defined.</b>

## DAFTAR TABEL

Tabel 2. 1 Contoh Cara Kerja OTP <i>Self-generate</i> ..	<b>Error! Bookmark not defined.</b>
Tabel 2. 2 Tabel Versi-versi AES.....	<b>Error! Bookmark not defined.</b>
Tabel 2. 3 Tabel S-Box AES (William Stalling).....	<b>Error! Bookmark not defined.</b>
Tabel 2. 4 Tabel Inverse S-Box AES (William Stalling)	<b>Error! Bookmark not defined.</b>
Tabel 2. 5 Contoh <i>Plaintext dan Key</i> .....	<b>Error! Bookmark not defined.</b>
Tabel 2. 6 Ekspansi Kunci untuk Contoh Algoritma AES	<b>Error! Bookmark not defined.</b>
Tabel 2. 7 Contoh Hasil Enkripsi AES.....	<b>Error! Bookmark not defined.</b>
Tabel 2. 8 Contoh Tabel <i>Hamming Weight</i> .....	<b>Error! Bookmark not defined.</b>
Tabel 2. 9 Tabel R (Nilai Kritis) $\alpha = 0,05$ (Sonjaya, 2007)	<b>Error! Bookmark not defined.</b>
Tabel 4. 1 Data Kode Otentikasi Media Sosial .....	<b>Error! Bookmark not defined.</b>
Tabel 4. 2 Kombinasi kunci dengan panjang kunci tertentu (Arora, 2012) ...	<b>Error! Bookmark not defined.</b>
Tabel 4. 3 Waktu yang diperlukan untuk membongkar pesan enkripsi (Arora, 2012) .....	<b>Error! Bookmark not defined.</b>
Tabel 4. 4 <i>Model</i> .....	<b>Error! Bookmark not defined.</b>
Tabel 4. 5 <i>Controller</i> .....	<b>Error! Bookmark not defined.</b>
Tabel 4. 6 <i>View</i> .....	<b>Error! Bookmark not defined.</b>
Tabel 4. 7 <i>Library</i> .....	<b>Error! Bookmark not defined.</b>
Tabel 4. 8 Pelaksanaan pengujian <i>black box</i> .....	<b>Error! Bookmark not defined.</b>
Tabel 4. 9 Pesan dan Kunci yang akan dienkripsi AES 256 <i>bits</i>	<b>Error! Bookmark not defined.</b>
Tabel 4. 10 Hasil Enkripsi AES 256 <i>bits</i> .....	<b>Error! Bookmark not defined.</b>
Tabel 4. 11 Avalanche effect dengan kunci heksadesimal semua '01' .....	<b>Error! Bookmark not defined.</b>

- Tabel 4. 12 Avalanche effect dengan kunci heksadesimal semua '10' ..... **Error! Bookmark not defined.**
- Tabel 4. 13 Avalanche effect dengan kunci heksadesimal semua '00' ..... **Error! Bookmark not defined.**
- Tabel 4. 14 Avalanche effect dengan kunci heksadesimal semua '11' ..... **Error! Bookmark not defined.**
- Tabel 4. 15 Avalanche effect dengan kunci 'ilmukomputerupi'**Error! Bookmark not defined.**
- Tabel 4. 16 Avalanche effect dengan kunci 'ilkom2011'**Error! Bookmark not defined.**
- Tabel 4. 17 Uji Keacakan dengan kunci kondisi pertama**Error! Bookmark not defined.**
- Tabel 4. 18 Uji Keacakan dengan kunci kondisi kedua**Error! Bookmark not defined.**
- Tabel 4. 19 Uji Keacakan dengan kunci kondisi ketiga**Error! Bookmark not defined.**
- Tabel 4. 20 Uji Keacakan dengan kunci kondisi keempat**Error! Bookmark not defined.**
- Tabel 4. 21 Uji Keacakan dengan kunci kondisi kelima**Error! Bookmark not defined.**
- Tabel 4. 22 Uji Keacakan dengan kunci kondisi kelima**Error! Bookmark not defined.**
- Tabel 4. 23 Hasil Uji Modifikasi AES 256 *bits*.....**Error! Bookmark not defined.**
- Tabel 4. 24 Hasil Avalanche Effect .....**Error! Bookmark not defined.**

## DAFTAR GAMBAR

- Gambar 2. 1 *CIA Triad* (William Staling. 2011)...**Error! Bookmark not defined.**
- Gambar 2. 2 *Diagram Proses Enkripsi dan Dekripsi AES* (William Staling. 2011)  
.....**Error! Bookmark not defined.**
- Gambar 2. 3 Perubahan *Plaintext* menjadi *Array State***Error! Bookmark not defined.**
- Gambar 2. 4 Struktur Data AES.....**Error! Bookmark not defined.**
- Gambar 2. 5 Contoh *Array State* dan kunci dalam notasi Heksadesimal ..... **Error! Bookmark not defined.**
- Gambar 2. 6 Proses Transformasi *SubBytes()* (William Stalling, 2011)..... **Error! Bookmark not defined.**
- Gambar 2. 7 Matriks Perhitungan S-Box (William Stalling, 2011)..... **Error! Bookmark not defined.**
- Gambar 2. 8 Diagram Pembuatan S-Box (William Stalling, 2011)..... **Error! Bookmark not defined.**
- Gambar 2. 9 Matriks Perhitungan *Inverse S-Box* (William Stalling, 2011) .. **Error! Bookmark not defined.**
- Gambar 2. 10 Diagram Pembuatan *Inverse S-Box* (William Stalling, 2011) **Error! Bookmark not defined.**
- Gambar 2. 11 Transformasi *ShiftRows()* .....**Error! Bookmark not defined.**
- Gambar 2. 12 Contoh Transformasi *ShiftRows()* ...**Error! Bookmark not defined.**
- Gambar 2. 13 Matriks Transformasi *MixColumns()***Error! Bookmark not defined.**
- Gambar 2. 14 Contoh Transformasi *MixColumns()* (William Stalling, 2011)**Error! Bookmark not defined.**
- Gambar 2. 15 Matriks Transformasi *Inverse MixColumns()* (William Stalling, 2011).....**Error! Bookmark not defined.**
- Gambar 2. 16 Contoh Transformasi *AddRoundKey()***Error! Bookmark not defined.**

Gambar 2. 17 Contoh Pergeseran ShiftRow Penelitian Sebelumnya ..... **Error! Bookmark not defined.**

Gambar 3. 1 Desain Penelitian..... **Error! Bookmark not defined.**

Gambar 3. 2 Model *Waterfall* (Sommerville, 2011)**Error! Bookmark not defined.**

Gambar 4. 1 Contoh Kode Otentikasi melalui SMS**Error! Bookmark not defined.**

Gambar 4. 2 Contoh Operasi XOR seluruh elemen kunci**Error! Bookmark not defined.**

Gambar 4. 3 Contoh Operasi XOR seluruh elemen S-Box dengan XOR\_kunci ..... **Error! Bookmark not defined.**

Gambar 4. 4 *Pseudocode* inverse S-Box ..... **Error! Bookmark not defined.**

Gambar 4. 5 Contoh menghitung peringkat tiap baris RoundKey pertama... **Error! Bookmark not defined.**

Gambar 4. 6 Pergeseran tiap baris State sesuai peringkat barisnya ..... **Error! Bookmark not defined.**

Gambar 4. 7 Rumus Permutasi..... **Error! Bookmark not defined.**

Gambar 4. 8 Membangkitkan Kode Otentikasi..... **Error! Bookmark not defined.**

Gambar 4. 9 Membongkar Kode Otentikasi ..... **Error! Bookmark not defined.**

Gambar 4. 10 Proses pengiriman SMS Kode Otentikasi**Error! Bookmark not defined.**

Gambar 4. 11 *Use Case* Aplikasi Registrasi *Online***Error! Bookmark not defined.**

Gambar 4. 12 Rancangan Basis Data..... **Error! Bookmark not defined.**

Gambar 4. 13 Tampilan Main Menu ..... **Error! Bookmark not defined.**

Gambar 4. 14 Tampilan Pilihan Algoritma AES 256 *bits***Error! Bookmark not defined.**

Gambar 4. 15 Contoh *Form* Enkripsi dan Dekripsi AES 256 *bits* ..... **Error! Bookmark not defined.**



- Gambar 4. 16 Contoh *Form* Enkripsi dan Dekripsi AES 256 bits ..... **Error!**  
**Bookmark not defined.**
- Gambar 4. 17 Contoh *Form* Enkripsi dan Dekripsi AES 256 bits ..... **Error!**  
**Bookmark not defined.**
- Gambar 4. 18 Tampilan *Form* Registrasi ..... **Error! Bookmark not defined.**
- Gambar 4. 19 Contoh Kode Otentikasi yang dikirimkan **Error! Bookmark not defined.**
- Gambar 4. 20 Tampilan *Form* Aktivasi ..... **Error! Bookmark not defined.**
- Gambar 4. 21 Tampilan *Form* Aktivasi ..... **Error! Bookmark not defined.**
- Gambar 4. 22 Tampilan Cryptool 1.4.3 ..... **Error! Bookmark not defined.**
- Gambar 4. 23 Tampilan Menu menuju *Randomness Test* **Error! Bookmark not defined.**
- Gambar 4. 24 Tampilan Eksekusi Contoh Tes *Randomness* **Error! Bookmark not defined.**
- Gambar 4. 25 Grafik hasil *Avalanche Effect* ..... **Error! Bookmark not defined.**