

DAFTAR ISI

PERNYATAAN.....	Error! Bookmark not defined.
ABSTRAK	Error! Bookmark not defined.
ABSTRACT	Error! Bookmark not defined.
KATA PENGANTAR	Error! Bookmark not defined.
UCAPAN TERIMA KASIH.....	Error! Bookmark not defined.
DAFTAR ISI.....	vii
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xi
BAB I PENDAHULUAN	Error! Bookmark not defined.
1.1. Latar Belakang	Error! Bookmark not defined.
1.2. Rumusan Masalah	Error! Bookmark not defined.
1.3. Tujuan Penelitian.....	Error! Bookmark not defined.
1.4. Batasan Masalah.....	Error! Bookmark not defined.
1.5. Sistematika Penulisan.....	Error! Bookmark not defined.
BAB II KAJIAN PUSTAKA	Error! Bookmark not defined.
2.1 Pengertian <i>Electronic mail</i> (Email).....	Error! Bookmark not defined.
2.2 Keamanan Informasi	Error! Bookmark not defined.
2.3 Kriptografi	Error! Bookmark not defined.
2.3.1. Algoritma Simetri	Error! Bookmark not defined.
2.3.2. Algoritma Asimetri	Error! Bookmark not defined.
2.4 Algoritma BC3	Error! Bookmark not defined.
2.4.1. <i>Substitution-box</i> (S-box).....	Error! Bookmark not defined.
2.4.2. Fungsi F	Error! Bookmark not defined.

2.4.3.	Fungsi FA dan FA^{-1}	Error! Bookmark not defined.
2.4.4.	Ekspansi Kunci (<i>Key Expansion/Key Schedule</i>)	Error! Bookmark not defined.
2.4.5.	<i>Randomizing</i> (Enkripsi/Dekripsi)	Error! Bookmark not defined.
2.5	Algoritma RSA	Error! Bookmark not defined.
2.5.1.	Pembangkitan Pasangan Kunci pada Algoritma RSA	Error! Bookmark not defined.
2.5.2.	Proses Enkripsi pada Algoritma RSA	Error! Bookmark not defined.
2.5.3.	Proses Dekripsi pada Algoritma RSA	Error! Bookmark not defined.
BAB III METODOLOGI PENELITIAN.....		Error! Bookmark not defined.
3.1.	Desain Penelitian	Error! Bookmark not defined.
3.2.	Metode Penelitian.....	Error! Bookmark not defined.
3.2.1.	Metode Pengumpulan Data.....	Error! Bookmark not defined.
3.2.2.	Metode Pengembangan Perangkat Lunak	Error! Bookmark not defined.
3.3.	Instrumen Penelitian	Error! Bookmark not defined.
3.3.1.	Alat Penelitian.....	Error! Bookmark not defined.
3.3.2.	Bahan Penelitian	Error! Bookmark not defined.
3.3.3.	Pengujian	Error! Bookmark not defined.
BAB IV HASIL PENELITIAN DAN PEMBAHASAN		Error! Bookmark not defined.
4.1.	Analisis dan Pembahasan	Error! Bookmark not defined.
4.1.1.	Pengumpulan Data Penelitian	Error! Bookmark not defined.

- 4.1.2. Penyandian Pesan Email menggunakan Kombinasi Dua Algoritma Kriptografi BC3 dan RSA.....**Error! Bookmark not defined.**
- 4.1.3. Pengiriman Email menggunakan Server G-Mail**Error! Bookmark not defined.**
- 4.1.4. Pendekripsian Pesan Email Terenkripsi menggunakan Kombinasi Dua Algoritma Kriptografi BC3 dan RSA.....**Error! Bookmark not defined.**
- 4.2. Pengembangan Perangkat Lunak**Error! Bookmark not defined.**
 - 4.2.1. Deskripsi Sistem**Error! Bookmark not defined.**
 - 4.2.2. Perancangan Sistem**Error! Bookmark not defined.**
 - 4.2.3. Implementasi Antarmuka.....**Error! Bookmark not defined.**
- 4.3. Pengujian**Error! Bookmark not defined.**
 - 4.3.1. Pengujian Proses Enkripsi dan Dekripsi**Error! Bookmark not defined.**
 - 4.3.2. Modifikasi *Ciphertext***Error! Bookmark not defined.**
 - 4.3.3. Modifikasi *Cipherkey***Error! Bookmark not defined.**
 - 4.3.4. Penggunaan Kunci Privat dari Pasangan Kunci RSA Lain **Error! Bookmark not defined.**
 - 4.3.5. Pengujian Lama Waktu Proses Enkripsi dan Dekripsi **Error! Bookmark not defined.**
- 4.4. Hasil Pengujian dan Pembahasan.....**Error! Bookmark not defined.**
 - 4.4.1. Implementasi Kombinasi Dua Algoritma Kriptografi, Algoritma BC3 dan Algoritma RSA, pada Sistem Keamanan Pesan Email **Error! Bookmark not defined.**
 - 4.4.2. Pengaruh Kombinasi Dua Algoritma Kriptografi, Algoritma BC3 dan Algoritma RSA, terhadap Dua Tujuan Kriptografi**Error! Bookmark not defined.**

4.4.3. Lama Waktu Proses Enkripsi dan Dekripsi **Error! Bookmark not defined.**

BAB V KESIMPULAN DAN SARAN.....**Error! Bookmark not defined.**

5.1. Kesimpulan.....**Error! Bookmark not defined.**

5.2. Saran**Error! Bookmark not defined.**

DAFTAR PUSTAKA**Error! Bookmark not defined.**

DAFTAR GAMBAR

- Gambar 2. 1 Proses Enkripsi dan Dekripsi Sederhana **Error! Bookmark not defined.**
- Gambar 2. 2 Proses Enkripsi dan Dekripsi Algoritma Asimetri **Error! Bookmark not defined.**
- Gambar 2. 3 Arsitektur Algoritma Kriptografi Simetri BC3 **Error! Bookmark not defined.**
- Gambar 2. 4 S-box (dalam hexadesimal).....**Error! Bookmark not defined.**
- Gambar 2. 5 S_0 (dalam hexadesimal).....**Error! Bookmark not defined.**
- Gambar 2. 6 S_1 (dalam hexadesimal).....**Error! Bookmark not defined.**
- Gambar 2. 7 S_2 (dalam hexadesimal).....**Error! Bookmark not defined.**
- Gambar 2. 8 S_3 (dalam hexadesimal).....**Error! Bookmark not defined.**
- Gambar 3. 1 Skema Desain Penelitian.....**Error! Bookmark not defined.**
- Gambar 3. 2 Tahap-tahapan metode *Linier Sequence (Waterfall)*..... **Error! Bookmark not defined.**
- Gambar 4. 1 Skema Proses Kombinasi Dua Algoritma Kriptografi **Error! Bookmark not defined.**
- Gambar 4. 2 Skema Penyandian Pesan**Error! Bookmark not defined.**
- Gambar 4. 3 Skema Pendekripsian Pesan**Error! Bookmark not defined.**
- Gambar 4. 4 Perancangan Diagram DFD level 1...**Error! Bookmark not defined.**
- Gambar 4. 5 Pengembangan Kunci RSA**Error! Bookmark not defined.**
- Gambar 4. 6 *Flowchart* Penyandian dan Pengiriman Pesan Email **Error! Bookmark not defined.**
- Gambar 4. 7 *Flowchart* Pendekripsian Pesan Terenkripsi **Error! Bookmark not defined.**
- Gambar 4. 8 Antarmuka Menu Utama.....**Error! Bookmark not defined.**
- Gambar 4. 9 Antarmuka Pembangkitan Kunci RSA **Error! Bookmark not defined.**
- Gambar 4. 10 Antarmuka Pengiriman Pesan**Error! Bookmark not defined.**

Gambar 4. 11 Antarmuka Masukan Kunci Publik RSA pada Pengiriman Pesan
.....**Error! Bookmark not defined.**

Gambar 4. 12 Contoh Antarmuka Hasil Pengiriman Pesan Email Terenkripsi
.....**Error! Bookmark not defined.**

Gambar 4. 13 Antarmuka Pendekripsian Pesan.....**Error! Bookmark not defined.**

Gambar 4. 14 Antarmuka Masukan Kunci Privat RSA**Error! Bookmark not defined.**

Gambar 4. 15 Hasil Dekripsi *Ciphertext* menjadi Pesan Asli**Error! Bookmark not defined.**

Gambar 4. 16 Hasil *Capture* Wireshark Data Terenkripsi**Error! Bookmark not defined.**

DAFTAR TABEL

- Tabel 1. 1 Perbandingan Hasil Kinerja Algoritma BC3 dan AES **Error! Bookmark not defined.**
- Tabel 1. 2 Perbandingan Waktu Performa Algoritma BC3..... **Error! Bookmark not defined.**
- Tabel 1. 3 Perbandingan Implementasi Algoritma Kriptografi pada Perangkat Lunak..... **Error! Bookmark not defined.**
- Tabel 4. 1 Proses Mencari Kunci Privat (d)..... **Error! Bookmark not defined.**
- Tabel 4. 2 Konversi String ke Bentuk Biner **Error! Bookmark not defined.**
- Tabel 4. 3 Variabel XR Dibagi Menjadi Empat..... **Error! Bookmark not defined.**
- Tabel 4. 4 Pengembangan S-box dikenakan Masukan x_0, x_1, x_2, x_3 **Error! Bookmark not defined.**
- Tabel 4. 5 Hasil dari Tahap Akhir pada Proses Ekspansi Kunci – Penyandian Pesan Email..... **Error! Bookmark not defined.**
- Tabel 4. 6 Proses Enkripsi Kunci BC3 menggunakan Algoritma RSA..... **Error! Bookmark not defined.**
- Tabel 4. 7 Konversi Biner ke Bentuk Desimal **Error! Bookmark not defined.**
- Tabel 4. 8 Proses Dekripsi Kunci BC3 Terenkripsi menggunakan Algoritma RSA **Error! Bookmark not defined.**
- Tabel 4. 9 Hasil dari Tahap Akhir pada Proses Ekspansi Kunci – Pendekripsian Pesan Email Terenkripsi **Error! Bookmark not defined.**
- Tabel 4. 10 Hasil Pengujian Proses Enkripsi dan Dekripsi..... **Error! Bookmark not defined.**
- Tabel 4. 11 Hasil Dekripsi dari Perubahan 1 Bit *Ciphertext*..... **Error! Bookmark not defined.**
- Tabel 4. 12 Hasil Dekripsi dari Pengurangan 1 Bit *Ciphertext*..... **Error! Bookmark not defined.**
- Tabel 4. 13 Hasil Dekripsi dari Penambahan 1 Bit *Ciphertext*..... **Error! Bookmark not defined.**

Tabel 4. 14 Hasil Pengujian dari Modifikasi *Ciphertext***Error! Bookmark not defined.**

Tabel 4. 15 Modifikasi *Cipherkey* yang digunakan pada Pengujian..... **Error! Bookmark not defined.**

Tabel 4. 16 Hasil Dekripsi dengan Adanya Modifikasi pada *Cipherkey*..... **Error! Bookmark not defined.**

Tabel 4. 17 Hasil Dekripsi dengan Pemakaian Kunci Privat RSA yang Lain**Error! Bookmark not defined.**

Tabel 4. 18 Hasil Pengujian Lama Waktu Proses Enkripsi**Error! Bookmark not defined.**

Tabel 4. 19 Rasio Jumlah Bit Pesan Sebelum dan Setelah Proses Enkripsi .. **Error! Bookmark not defined.**

Tabel 4. 20 Hasil Penyederhanaan Rasio**Error! Bookmark not defined.**

Tabel 4. 21 Hasil Pengujian Lama Waktu Proses Dekripsi**Error! Bookmark not defined.**

Tabel 4. 22 Hasil Pengujian terhadap Tujuan Kriptografi Kerahasiaan **Error! Bookmark not defined.**