

DAFTAR ISI

COVER.....	i
LEMBAR PENGESAHAN	ii
LEMBAR ORISINALITAS	iii
ABSTRAK	iv
ABSTRACT	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xi
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	4
1.3. Batasan masalah.....	4
1.4. Tujuan	5
1.5. Manfaat	5
1.6. Rencana Kegiatan	6
1.6.1. Identifikasi Masalah.....	7
1.6.2. Studi Literatur	8
1.6.3. Perancangan	8
1.6.4. Pengujian dan Analisis.....	9
1.6.5. Penyimpulan Hasil	9
BAB II TINJAUAN PUSTAKA.....	10
2.1. Penelitian terdahulu.....	10
2.2. Landasan Teori	14
2.2.1. Kriptografi.....	14
2.2.2. Layanan Kriptografi	15
2.2.3. Kriptografi Modern	17
2.2.4. Algoritma Kriptografi Kunci-Simetri	17
2.2.5. <i>Cipher</i> Alir	19
2.2.6. Salsa20	19
2.2.7. SHA-256	36
2.2.8. File Transfer Protocol (FTP).....	36

2.2.9. Unified Modeling Language (UML).....	37
BAB III PERANCANGAN SISTEM	39
3.1. Deskripsi Sistem	39
3.2. Alat dan Bahan.....	40
3.2.1. Alat.....	40
3.2.2. Bahan.....	40
3.3. Perancangan	42
3.3.1. Desain dan Analisis Sistem.....	42
3.3.2. Implementasi Pembuatan Program	48
3.3.3. Konfigurasi Server	49
3.2. Deskripsi Pengujian dan Analisis	51
3.3.4. Pengujian Fungsionalitas Program.....	51
3.3.5. Pengujian <i>Sniffing Attack</i>	51
3.3.6. Pengujian <i>Known-plaintext Attack</i>	51
3.3.7. Pengujian <i>Avalanche Effect</i>	53
BAB IV HASIL DAN PEMBAHASAN	54
4.1. Skenario Pengujian	54
4.1.1. Skenario Pengujian Fungsionalitas Program	54
4.1.2. Skenario Pengujian <i>Sniffing Attack</i>	55
4.1.3. Skenario Pengujian <i>Known-plaintext Attack</i>	56
4.1.4. Skenario Pengujian <i>Avalanche Effect</i>	58
4.2. Hasil Pengujian	59
4.2.1. Hasil Pengujian Fungsionalitas	59
4.2.2. Hasil Pengujian <i>Sniffing Attack</i>	70
4.2.3. Hasil Pengujian <i>Known-plaintext Attack</i>	78
4.2.4. Hasil Pengujian <i>Avalanche Effect</i>	84
BAB V KESIMPULAN DAN SARAN	88
5.1. Kesimpulan	88
5.2. Saran	89
DAFTAR PUSTAKA	90