

DAFTAR ISI

LEMBAR PENGESAHAN	i
ABSTRAK	ii
ABSTRACT	iii
KATA PENGANTAR	iv
UCAPAN TERIMA KASIH	v
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
DAFTAR SINGKATAN	xii
DAFTAR ISTILAH	xiii
DAFTAR LAMPIRAN	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Tujuan Tugas Akhir	1
1.3 Rumusan Masalah	2
1.4 Batasan Masalah	2
1.5 Metode Penelitian	3
1.6 Sistematika Penulisan	3
BAB 2 DASAR TEORI	5
2.1 Sistem Kriptografi	5
2.1.1 Definisi Kriptografi	5
2.1.2 Algoritma Kriptografi Simetris	6
2.1.3 Stream Cipher	7
2.1.4 Avalanche Effect	7
2.2 Sistem Keamanan Universal Mobile Telecommunication System	7
2.2.1 Fitur Keamanan UMTS	7
2.2.2 Arsitektur Jaringan UMTS	8
2.2.2.1 User Equipment(UE)	8
2.2.2.1.1 Mobile Equipment	9
2.2.2.1.2 Universal Subscriber Identity Module	9

	2.2.2.2 UMTS Radio Access Network (UTRAN)	10
	2.2.2.3 Home Network	10
	2.2.2.3.1 Home Location Register (HLR)	10
	2.2.2.3.2 Authentication Centre (AUC)	10
	2.2.2.4 Visited Network	11
	2.2.2.4.1 Visitor Location Register (VLR)/SGSN	11
	2.2.3 Proses Autentikasi UMTS	12
	2.2.4 Algoritma Confidentiality dan Integrity	13
	2.2.4.1 Algoritma f8	14
	2.2.4.2 Algoritma f9	14
	2.2.5 Algoritma KASUMI	15
BAB III	PERANCANGAN SIMULASI ALGORITMA f8 DAN f9	19
	3.1 Perancangan Algoritma f8	19
	3.2 Perancangan Algoritma f9	20
	3.3 Pembangkitan Kunci	21
	3.3.1 Cipher Key(CK)	21
	3.3.2 Integrity Key(IK)	22
	3.4 Blok Diagram Proses Algoritma f8 dan f9	23
	3.5 Proses Simulasi Algoritma f8 dan f9(Pengirim)	24
	3.6 Proses Simulasi Algoritma f8 dan f9(Penerima)	25
	3.7 Perancangan Simulasi Kriptografi Algoritma f8 dan f9	26
	3.8 Tampilan Program	27
	3.8.1 Program Algoritma f8 dan f9	27
	3.8.2 Program Avalanche Effect	27
	3.9 Penggunaan Program	28
BAB IV	HASIL DAN ANALISA	30
	4.1 Sistem Simulator	30
	4.1.1 Sistem Operasi	30
	4.1.2 Bahasa Pemrograman	30
	4.1.3 Sistem Perangkat Keras	30
	4.2 Analisis Unjuk Kerja Algoritma f8 dan f9	31
	4.2.1 Proses Enkripsi Algoritma f8 dan f9	31

4.2.1.1 Text	31
4.2.1.2 Suara	32
4.2.1.3 Gambar	33
4.2.2 Proses Dekripsi Algoritma f8 dan f9	34
4.2.2.1 Text	34
4.2.2.2 Suara	35
4.2.2.3 Gambar	36
4.2.3 Perubahan Bit (Input/Output)	37
4.2.4 Avalanche Effect	37
4.2.4.1 Perubahan Satu Bit Plaintext	38
4.2.4.2 Perubahan Satu Bit Kunci	38
4.2.5 Perubahan Besar File	39
4.2.6 Waktu dan Performansi Proses	39
4.2.6.1 Text	40
4.2.6.2 Suara	40
4.2.6.3 Gambar	40
4.2.7 Ketahanan Terhadap Brute Force Attack	41
BAB V KESIMPULAN DAN SARAN	42
5.1 Kesimpulan	42
5.2 Saran	42
DAFTAR PUSTAKA	43
LAMPIRAN	