



DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN	iii
HALAMAN PERSEMBAHAN	iv
HALAMAN MOTTO	v
PRAKATA	vi
DAFTAR ISI	viii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
DAFTAR LAMBANG	xii
INTISARI	xiii
ABSTRACT	xiv
I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Pembatasan Masalah	2
1.4. Tujuan dan Manfaat Penelitian	2
1.5. Tinjauan Pustaka	3
1.6. Metodologi Penelitian	3
1.7. Sistematika Penulisan	4
II DASAR TEORI	5
2.1. Kriptografi	5
2.1.1. Sejarah Kriptografi	7
2.1.2. Sistem Kripto	8
2.1.3. Kriptografi Simetris	9
2.1.4. Stream Cipher Sinkron (Synchronous stream ciphers)	13
2.1.5. Stream Cipher Asinkron (Asynchronous stream ciphers)	15
2.1.6. Kriptografi Asimetris / Kunci Publik	17
2.2. Bilangan Bulat	18
2.2.1. Keterbagian	18
2.2.2. Algoritma Pembagian pada Bilangan Bulat	20
2.2.3. Representasi Bilangan Bulat	21
2.2.4. Persamaan Kongruen	24



2.3.	Struktur Aljabar	26
2.3.1.	Grup	26
2.3.2.	Ring	30
2.3.3.	Ring Polinomial	33
2.3.4.	Algoritma XOR	39
III	T-FUNCTION	40
3.1.	T-function	40
3.2.	Generator <i>Keystream</i> Acak Semu	47
3.3.	Feedback Shift Register	51
3.3.1.	Linear Feedback Shift Register (LFSR)	52
3.3.2.	Stream Cipher berdasarkan LFSR	60
3.4.	Clock Controlled Generator	61
3.4.1.	Generator Penyusutan (Shrinking Generator)	61
3.4.2.	Generator Langkah Bolak-Balik (Alternating Step Generator)	65
IV	T-FUNCTION SEBAGAI GENERATOR KEYSTREAM	71
4.1.	Kontruksi T-function sebagai Generator <i>Keystream</i>	71
4.2.	Analisa <i>T-function</i> Menggunakan Postulate Keacakan Golomb	74
4.2.1.	Evaluasi menggunakan Postulate 1	75
4.2.2.	Evaluasi menggunakan Postulate 2	75
4.2.3.	Evaluasi menggunakan Postulate 3	76
4.2.4.	Enkripsi dan Deskripsi pada Stream Cipher	78
V	KESIMPULAN	80
	DAFTAR PUSTAKA	82
A	TABEL KODE ASCII	83