

DAFTAR ISI

LEMBAR PENGESAHAN	i
BUKU CAPSTONE DESIGN.....	i
LEMBAR PERNYATAAN ORISINALITAS.....	ii
LEMBAR PERNYATAAN ORISINALITAS.....	iii
LEMBAR PERNYATAAN ORISINALITAS.....	iv
LEMBAR PERNYATAAN ORISINALITAS.....	v
ABSTRAK	vi
ABSTRACT.....	vii
KATA PENGANTAR.....	viii
UCAPAN TERIMA KASIH	ix
DAFTAR ISI.....	xi
DAFTAR GAMBAR.....	xv
DAFTAR TABEL	xvi
DAFTAR SINGKATAN.....	xvii
BAB 1 USULAN GAGASAN.....	1
1.1 Deskripsi Umum Masalah.....	1
1.2 Analisis Masalah	2
1.2.1 Aspek Ekonomi	2
1.2.2 Aspek Manufakturabilitas	3
1.2.3 Aspek Teknis	3
1.2.4 Aspek Keamanan	3
1.2.5 Aspek Lingkungan	3
1.3 Analisis Solusi yang Ada	4
1.3.1 Jenis Operasi yang Diterapkan.....	4
1.3.2 Jumlah Kunci yang Digunakan	4

1.3.3	Metode Dalam Pemrosesan Data.....	4
1.4	Tujuan Tugas Akhir	5
1.4.1	Tujuan umum.....	5
1.4.2	Tujuan Khusus.....	5
1.5	Batasan Tugas Akhir	6
BAB 2	TINJAUAN PUSTAKA	7
2.1	Teori Dasar	7
2.1.1	<i>Internet of Things</i>	7
2.1.2	Komunikasi <i>Machine-to-Machine</i> (M2M)	7
2.1.3	Konsep Dasar Kriptografi.....	7
2.2	Algoritma yang Digunakan.....	8
2.2.1	ASCON.....	9
2.2.2	PRESENT	9
2.2.3	LED	10
2.2.4	TWINE.....	12
2.3	Penelitian Terdahulu (<i>Related Work</i>).....	13
BAB 3	SPESIFIKASI DAN DESAIN SISTEM	15
3.1	Spesifikasi Sistem	15
3.1.1	<i>Privacy/Confidentiality</i>	15
3.1.2	<i>Integrity</i>	15
3.1.3	<i>Authentication</i>	15
3.1.4	<i>Availability</i>	15
3.1.5	<i>Access Control</i>	16
3.2	Desain Sistem.....	16
3.3	Metode Pengukuran yang Sesuai dengan Solusi Terpilih.....	18
3.3.1	Confusion & Diffusion (Avalanche Effect)	18
3.3.2	Waktu Enkripsi & Dekripsi.....	19

3.3.3	Tingkat Kerumitan (<i>Big O Complexity</i>)	19
3.3.4	Instruksi Mesin.....	20
3.3.5	Penggunaan Memori.....	20
3.3.6	<i>Hamming Distance</i>	20
BAB 4 IMPLEMENTASI		21
4.1	Deskripsi umum implementasi	21
4.1.1	Proses Enkripsi.....	22
4.1.2	Proses Dekripsi.....	22
4.2	Detail Implementasi.....	23
4.2.1	ASCON.....	23
4.2.2	PRESENT	24
4.2.3	LED	25
4.2.4	TWINE.....	26
4.3	Prosedur Pengoperasian Solusi	27
4.3.1	Persiapan Komponen dan Pemrograman	27
4.3.2	Perancangan dan Konfigurasi Rangkaian	27
4.3.3	Tahapan Operasi Sistem	28
4.3.4	Hasil yang Ditampilkan.....	28
BAB 5 31		
PENGUJIAN		31
5.1	Skema Pengujian Sistem	31
5.2	Proses Pengujian dan Analisis Hasil	31
5.2.1	Proses Pengujian dan Analisis Confusion dan Diffusion	31
5.2.2	Kecepatan Komputasi	40
5.2.3	Kompleksitas Algoritma (<i>Big O</i>)	44
5.2.4	Instruksi Mesin.....	51
5.2.5	Pengukuran Memori.....	60

5.2.6	Analisa Hasil Pengujian	65
5.2.7	Rangkuman Hasil Pengujian	76
5.2.8	Rencana Pengembangan Berkelanjutan.....	77
BAB 6 78		
KESIMPULAN DAN SARAN		78
6.1	Kesimpulan.....	78
6.2	Saran	79
DAFTAR PUSTAKA.....		81
LAMPIRAN.....		85