

DAFTAR ISI

HALAMAN JUDUL.....	i
LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN ORISINALITAS	iii
ABSTRACT.....	iv
ABSTRAK	v
KATA PENGANTAR	vi
UCAPAN TERIMA KASIH.....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	1
1.3 Batasan Masalah.....	2
1.4 Tujuan dan Manfaat	2
1.5 Metodologi	2
1.6 Penelitian Terdahulu	3
BAB II DASAR TEORI	4
2.1 RSA.....	4
2.1.1 Properti algoritma RSA	4
2.1.2 Algoritma Membangkitkan Pasangan Kunci RSA.....	4
2.1.3 Algoritma Enkripsi/Dekripsi RSA	6
2.1.4 Keamanan RSA	7
2.2 Modifikasi RSA menggunakan metode <i>n-prime</i>	8
2.3 Avalanche effect.....	10
BAB III PERANCANGAN SISTEM	11
3.1. Deskripsi Sistem.....	11
3.2. Perancangan Sistem Pembangkitan Pasangan Kunci Modifikasi RSA	13
3.2.1. Masukan nilai <i>n-prime</i>	14
3.2.2. Masukan nilai bilangan prima p_i dimana $i = 1$ sampai dengan np	14

3.2.3.	Menghitung nilai n dan $\phi(n)$	14
3.2.4.	Masukan nilai e dimana $1 < e < \phi(n)$ dan $\text{gcd}(e, \phi(n)) = 1$	14
3.2.5.	Menghitung nilai d	14
3.2.6.	Keluaran pasangan kunci	15
3.3.	Perancangan Sistem Enkripsi Modified RSA	15
3.3.1.	Proses Konversi Message – Angka	15
3.3.2.	Proses Otentikasi	16
3.3.3.	Proses Pengecekan dan Pembagian Blok Baru	16
3.3.4.	Proses Enkripsi	16
3.3.5.	Proses Konversi Angka – Ciphertext	17
3.4.	Perancangan Sistem Dekripsi Pesan	17
3.4.1.	Proses Konversi Ciphertext – Angka	18
3.4.2.	Proses Dekripsi	18
3.4.3.	Proses Pengecekan dan Pembagian Blok Baru	18
3.4.4.	Proses Otentikasi	19
3.4.5.	Proses Konversi Angka – Message	19
3.5.	Skenario Pengujian Sistem	19
BAB IV PENGUJIAN DAN ANALISIS		21
4.1	Hasil Pengujian Sistem Pembangkitan Pasang Kunci Modified RSA	21
4.1.1.	Pengujian masukan p_i bukan bilangan prima	21
4.1.2.	Pengujian masukan nilai e bukan bilangan relatif prima terhadap $\phi(n)$	22
4.1.3.	pengujian penarikan data sample keluaran sistem pembangkitan pasangan kunci modified RSA	22
4.1.4.	Pengujian Brute Force Attack	23
4.2	Hasil Pengujian Sistem Enkripsi Modified RSA	24
4.2.1.	Pengujian sistem enkripsi modified RSA dan proses yang terjadi didalamnya	24
4.2.2.	Pengujian pengaruh n-prime pada sistem enkripsi	27
4.2.3.	Pengujian waktu performansi pada sistem enkripsi	29
4.2.4.	Pengujian Avalanche Effect pada sistem enkripsi	32

4.2.5. Pengujian Chi-Square	40
4.3 Hasil Pengujian Sistem Dekripsi Modified RSA	42
4.3.1. Pengujian Sistem Dekripsi Modified RSA dan Proses yang Terjadi Didalamnya.....	42
4.3.2. Pengujian pengaruh pengirim pada sistem dekripsi modified RSA	43
4.3.3. Pengujian waktu performansi pada sistem dekripsi modified RSA	45
4.3.4. Pengujian Avalanche Effect pada sistem dekripsi.....	47
BAB V KESIMPULAN DAN SARAN.....	51
5.1 Kesimpulan.....	51
5.2 Saran.....	51
DAFTAR PUSTAKA	52
LAMPIRAN A DATA PENGUJIAN	A-1
1. Tabel Mapping Angka - Message	A-1
2. Tabel Mapping Angka - Ciphertext	A-2
3. Tabel ASCII	A-5
4. Tabel Chi-Square.....	A-8