

DAFTAR ISI

<i>ABSTRACT</i>	iv
ABSTRAK	v
MOTTO DAN PERSEMBAHAN	vi
KATA PENGANTAR.....	vii
DAFTAR ISI	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN	xiii
BAB I PENDAHULUAN.....	I-1
1.1 Latar Belakang	I-1
1.2 Rumusan Masalah	I-5
1.3 Tujuan Penelitian.....	I-6
1.4 Manfaat Penelitian.....	I-6
1.5 Batasan Masalah.....	I-7
BAB II LANDASAN TEORI	II-1
2.1 Kriptografi.....	II-1
2.2 Kriptografi Simetris dan Asimetris.....	II-2
2.3 Lattice Based Cryptography	II-4
2.4 Number Theoretic Transform (NTT)	II-6
2.5 Karatsuba	II-8
2.6 Kundu's Hybridized Karatsuba-NTT Algorithm	II-9
2.7 Nth Degree Truncated Polynomial Ring Units (NTRU)	II-12
2.8 State Of The Art	II-13

2.9	Matriks Penelitian.....	II-16
BAB III METODOLOGI		III-1
3.1	Metodologi.....	III-1
BAB IV HASIL DAN PEMBAHASAN		IV-1
4.1	Hasil Bit Keamanan.....	IV-1
4.2	Hasil Kompresi Ukuran kunci dan Ciphertext	IV-5
4.3	Hasil Penggunaan Bandwith	IV-7
4.4	Hasil Operasi Polinomial	IV-1
4.5	Hasil Algoritma NTRU.....	IV-8
4.6	Hasil Keseluruhan	IV-10
BAB V KESIMPULAN DAN SARAN.....		V-1
5.1	Kesimpulan	V-1
5.2	Saran	V-3
DAFTAR PUSTAKA.....		V-1

DAFTAR TABEL

Tabel 2.1 State Of The Art.....	II-13
Tabel 2.2 Matriks Penelitian.....	II-16
Tabel 4.1 Estimasi Bit Keamanan.....	IV-4
Tabel 4.2 Perbandingan Besaran Nilai Kunci dan Ciphertext.	IV-6
Tabel 4.3 Perbandingan Bandwidth	IV-7
Tabel 4.4 Hasil Implementasi (average 10.000)	IV-1
Tabel 4.5 Perbandingan Kecepatan Setiap Metode	IV-2
Tabel 4.6 Hasil Keygen, enkrip, dan dekrip	IV-8
Tabel 4.7 Perbandingan Akhir Eksperimen.....	IV-11

DAFTAR GAMBAR

Gambar 2.1 Taxonomy Kriptografi (Maqsood et al., 2017).....	II-1
Gambar 2.2 Kriptografi Simetris	II-3
Gambar 2.3 Kriptografi Asimetris	II-3
Gambar 2.4 Contoh Kisi Benar	II-5
Gambar 2.5 Contoh Kisi Salah	II-6
Gambar 3.1 Metode Perkalian	III-2
Gambar 3.2 Metode Yang Digunakan.....	III-4
Gambar 3.3 Flowchart Algoritma NTRU.....	III-5
Gambar 3.4 Fungsi Parameter	III-6

DAFTAR LAMPIRAN

Lampiran 1. Pseudocode	V-6
Lampiran 2. Surat Keterangan Tugas Akhir	V-10
Lampiran 3. Lembar Revisi Usulan Penelitian Pembimbing 1	V-11
Lampiran 4. Lembar Revisi Usulan Penelitian Pembimbing 2	V-12
Lampiran 5. Lembar Revisi Usulan Penelitian Penguji 1	V-13
Lampiran 6. Lembar Revisi Usulan Penelitian Penguji 2	V-14
Lampiran 7. Lembar Konsultasi Pembimbing 1	V-15
Lampiran 8. Lembar Konsultasi Pembimbing 2	V-16
Lampiran 9. Lembar Mengikuti Sidang Seminar Hasil	V-17
Lampiran 10. Lembar Rekap Perbaikan	V-18