

DAFTAR ISI

DAFTAR ISI.....	iv
DAFTAR GAMBAR	vi
DAFTAR TABEL.....	viii
INTISARI.....	1
ABSTRACT.....	2
BAB I	3
1.1. Latar Belakang	3
1.2. Rumusan Masalah	5
1.3. Batasan Masalah.....	5
1.4. Tujuan Penelitian.....	6
1.5. Manfaat Penelitian.....	6
1.6. Metodologi Penelitian	6
1.7. Sistematika Penulisan.....	8
BAB II.....	10
BAB III	19
3.1. Hardware Security Module.....	19
3.2. Kriptografi	22
3.2.1 Advanced Encryption Standard (AES)	23
SubByte (Substitusi Byte).....	24
ShiftRow (Pergeseran Baris)	24
MixColumns (Pencampuran Kolom).....	24
AddRoundKey (Penambahan Kunci)	25
3.2.2 Rivest-Shamir-Adleman (RSA)	27
3.3. Key Management System.....	32
3.4. SoftHSM.....	33
3.5. Single Board Computer	34
BAB IV	36
4.1. Analisis Sistem	36
4.2. Tahapan Penelitian	37



4.3.	Perancangan Sistem.....	38
4.3.1.	Pembuatan Algoritma Kriptografi.....	40
4.3.2.	Implementasi SoftHSM.....	42
4.4.	Rancangan Pengujian Sistem	44
4.5.	Alat dan Bahan	46
BAB V	49
5.1	Implementasi Sistem Enkripsi Ganda	49
5.2	Implementasi Algoritma Kriptografi AES	49
5.2	Implementasi Algoritma Kriptografi RSA (Enkripsi).....	53
5.4	Implementasi SoftHSM	57
5.5	Implementasi Algoritma Kriptografi RSA (Dekripsi).....	59
5.6	Implementasi Algoritma Kriptografi AES (Dekripsi).....	61
5.7	Implementasi pada Perangkat Keras	65
BAB VI	66
6.1	Pengujian Time Consumption	66
6.2	Pengujian Memory Consumption.....	71
6.3	Pengujian Power Current.....	74
6.4	Pengujian Keamanan Slot SoftHsm dengan <i>Attacking Key Extraction</i> .76	
6.5	Hasil Data Pemrosesan	78
BAB VII	81
7.1	Kesimpulan.....	81
7.2	Saran	82
DAFTAR PUSTAKA	83

DAFTAR GAMBAR

Gambar 3.1 Skema HSM dengan Arduino(Prawira P et al., 2020)	21
Gambar 3.2 HSM yang terkoneksi dengan internet(Luo et al., 2018)	21
Gambar 3.3 Mekanisme proses kriptografi	22
Gambar 3.4 Sistem kerja Algoritma AES	26
Gambar 3.5 Sistem Kerja Algoritma RSA	28
Gambar 3.6 Sistem KMS secara keseluruhan (Kuzminykh et al., 2020).....	33
Gambar 3.7 Model General PKCS#11	34
Gambar 3.8 Contoh <i>single board computer</i>	35
Gambar 4.1 Desain Keseluruhan Sistem.....	37
Gambar 4.2 Tahapan Penelitian	37
Gambar 4.3 Rancangan Sistem <i>hardware security module</i>	38
Gambar 4.4 Proses enkripsi berlapis ganda	39
Gambar 4.5 Skema Teknis Perancangan HSM keseluruhan.....	39
Gambar 4.6 Sistem Algoritma Kriptografi Enkripsi Ganda.....	41
Gambar 4.7 Ilustrasi sistem SoftHSM dalam HSM yang dirancang	43
Gambar 4.8 Bentuk Slot pada SoftHSM	43
Gambar 4.9 Perhitungan CPU dan memory pada Htop	45
Gambar 4.10 Pengujian power (Yilmaz & Ozdemir, 2018)	46
Gambar 5. 1 Proses Enkripsi Menggunakan Algoritma AES	52
Gambar 5. 2 Proses Pembangkit Kunci RSA.....	54
Gambar 5. 3 Proses Enkripsi menggunakan Algoritma RSA	56
Gambar 5. 4 Interface SoftHSM	57
Gambar 5. 5 Proses Pembuatan Slot SoftHSM.....	58
Gambar 5. 6 Proses memasukkan kunci ke dalam Slot SoftHSM	58
Gambar 5. 7 List Kunci di dalam Slot SoftHSM	58
Gambar 5. 8 Alur Kerja Slot SoftHSM.....	59
Gambar 5. 9 Alur Dekripsi RSA.....	61
Gambar 5. 10 Alur Dekripsi AES	64
Gambar 5. 11 Proses <i>deployment</i> seluruh pemrogram ke dalam jetson Nano ...	65



Gambar 6. 1 Testing <i>power consumption</i> dengan USB power tester	74
Gambar 6. 2 Ilustrasi Sistem Pengujian	77
Gambar 6. 3 Proses <i>attacking key extraction</i>	77
Gambar 6. 4 Hasil <i>attacking key extraction</i>	77



DAFTAR TABEL

Tabel 2.1 Komparasi Algoritma Kriptografi (Jaspin et al., 2021)	13
Tabel 4.1 Rencana Pengujian.....	45
Tabel 4.2 Daftar Alat.....	47
Tabel 4.3 Bahan yang digunakan	48