

**ANALISIS *SIDE CHANNEL ATTACK* PADA PENGAMANAN
APLIKASI E-VOTING MENGGUNAKAN ALGORITMA
*PAILLIER***



Skripsi

Untuk memenuhi syarat memperoleh Derajat
Sarjana Teknik (S.T.)

Oleh:

AGNES GABRIELLA MANIK

NIM 2001020043

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2024**

**ANALISIS *SIDE CHANNEL ATTACK* PADA PENGAMANAN
APLIKASI E-VOTING MENGGUNAKAN ALGORITMA
*PAILLIER***



Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D.
NIDN. 0002048401






Nurul Hayaty, S.T., M.Cs
NIDN. 0027039101

HALAMAN PENGESAHAN

Judul Skripsi : Analisis Side Channel Attack Pada Pengamanan Aplikasi E-Voting Menggunakan Algoritma Paillier
Nama Mahasiswa : Agnes Gabriella Manik
NIM : 2001020043
Jurusan : Teknik Informatika

Telah dipertahankan di depan Dewan Penguji dan dinyatakan lulus pada tanggal 22 Juli 2024

Susunan Tim Pembimbing dan Penguji


Jabatan	Nama Dosen	Tanda Tangan	Tanggal
Pembimbing I	: Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D		29/07/24
Pembimbing II	: Nurul Hayaty, S.T., M.Cs		29/07/24
Ketua Penguji	: Tekad Matulatan, S.Sos., S.Kom., M.Inf.Tech		24/07/2024
Anggota Penguji I	: Muhamad Radzi Rathomi, S.Kom., M.Cs		25/7/24
Anggota Penguji II	: Novrizal Fattah Fahmitra, S.Kom., M.Kom		25/07/2024

Tanjungpinang, 30 Juli 2024

Universitas Maritim Raja Ali Haji

Dekan Fakultas Teknik dan Teknologi Kemaritiman




I. Sapta Nugraha, S.T., M.Eng

NIP 198904132015041005

PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan skripsi dengan judul *Analisis Side Channel Attack Pada Pengamanan Aplikasi E-Voting Menggunakan Algoritma Paillier* adalah benar hasil karya saya dengan bimbingan serta arahan dari dosen pembimbing dan belum ada diajukan dengan bentuk apa pun kepada universitas mana pun. Sumber informasi yang dikutip dari karya yang telah diterbitkan ataupun tidak diterbitkan dari penulis lain sudah disebutkan didalam teks dan dicantumkan kedalam Daftar Pustaka pada bagian akhir skripsi.

Apabila kemudian hari terbukti bahwa pernyataan saya tidak benar dan juga melanggar peraturan yang sah pada karya tulis dan hak intelektual, maka saya bersedia ijazah yang sudah saya terima untuk diambil kembali oleh pihak Universitas Maritim Raja Ali Haji.

Tanjungpinang, 01 Juli 2024

Yang menyatakan



Agnes Gabriella Manik

KATA PENGANTAR

Puji dan Syukur penulis panjatkan atas kehadiran Tuhan Yang Maha Esa yang telah memberikan karunia, serta rahmat-Nya kepada penulis, sehingga dapat menyelesaikan skripsi yang berjudul “Analisis *Side Channel Attack* Pada Pengamanan Aplikasi E-Voting Menggunakan Algoritma *Paillier*”.

Penulisan skripsi bertujuan untuk memperoleh salah satu persyaratan gelar Sarjana Teknik (S.T) pada Program Studi Teknik Informatika Fakultas Teknik dan Teknologi Kemaritiman Universitas Maritim Raja Ali Haji. Dalam penulisan skripsi tentu mengalami banyak kendala yang dihadapi dan dapat diselesaikan atas bantuan pihak-pihak terkait.

Penulis menyampaikan penghargaan setinggi-tingginya untuk semua pihak yang telah membantu serta memberikan dukungan, bimbingan, dan motivasi pada penulisan skripsi. Untuk ini penulis menyampaikan ucapan terimakasih kepada:

1. Segala pujian dan kemuliaan bagi Tuhan Yesus Kristus atas segala berkat, kasih karunia, serta penyertaan-Nya sepanjang perjalanan hidup dan studi saya.
2. Orang Tua tercinta yaitu Bapak Hotman Manik dan Ibu Eva Farida Haloho serta saudara-saudara saya yang telah mendoakan serta memberikan semangat dan juga dukungan sehingga menjadi sumber kekuatan dalam kesulitan-kesulitan yang ditemui pada saat penelitian tugas akhir.
3. Prof. Dr. Agung Dhamar Syakti, S.Pi., DEA. Selaku Rektor Universitas Maritim Raja Ali Haji (UMRAH) yang berperan aktif dan juga berkontribusi untuk mendukung kegiatan-kegiatan akademik demi memajukan Universitas Maritim Raja Ali Haji (UMRAH).
4. Bapak Ir. Sapta Nugraha, S.T., M.Eng. selaku Dekan Fakultas Teknik dan Teknologi Kemaritiman Universitas Maritim Raja Ali Haji.
5. Bapak Muhamad Radzi Rathomi, S.kom., M.Cs selaku Ketua Jurusan Teknik Informatika Universitas Maritim Raja Ali Haji(UMRAH).
6. Bapak Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D. selaku pembimbing I yang dapat menyediakan tenaga dan pikiran serta waktu untuk bimbingan ketika penyusunan skripsi.

7. Ibu Nurul Hayaty, S.T., M.Cs selaku pembimbing II yang menyediakan waktu, tenaga dan juga pikiran serta membimbing penyusunan skripsi.
8. Dosen penguji karena telah memberikan masukan, kritik, serta saran untuk penelitian.
9. Kepada seluruh Dosen dan Staff Universitas Maritim Raja Ali Haji (Umrah) terkhusus Jurusan Teknik Informatika karena telah memberikan ilmu melalui perkuliahan dan membantu serta membimbing selama berada di Universitas Maritim Raja Ali Haji (UMRAH).
10. Teman-teman seperjuangan Angkatan 2020 Program Studi Teknik Informatika yang saling membantu dan memberikan keceriaan serta kebersamaan yang tak ternilai.

Penulis menyadari bahwa penulisan pada skripsi ini jauh dari sempurna, oleh karena itu penulis menerima kritik maupun saran yang dapat membangun dari pembaca untuk kesempurnaan dan perbaikan serta harapan pada skripsi ini bisa memberikan banyak manfaat untuk para pembaca.

Tanjungpinang, 01 Juli 2024



(Agnes Gabriella Manik)

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
PERNYATAAN ORISINALITAS	iv
HALAMAN PERSEMBAHAN	v
HALAMAN MOTO	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
GLOSARIUM	xiii
ABSTRAK	xiv
ABSTRACT	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	4
BAB II KAJIAN LITERATUR	6
2.1 Tinjauan Pustaka	6
2.2 Landasan Teori	9
2.2.1 Pengertian e-voting	9
2.2.2 Kriptografi	9
2.2.3 Enkripsi Homomorfik	10
2.2.4 Algoritma <i>Paillier</i>	12
2.2.5 <i>Side Channel Attack</i>	15
2.2.6 <i>Timing Attack</i>	15
BAB III METODE PENELITIAN	17
3.1 Waktu Penelitian	17
3.2 Tahapan Penelitian	17
3.3 Jenis Penelitian	19
3.4 Analisis Dan Perancangan	19
3.4.1 Analisis Data	19
3.4.2 Perancangan Algoritma <i>Paillier</i>	19
3.5 Implementasi	23
3.5.1 Algoritma <i>Paillier</i>	25
3.5.2 <i>Timing Attack</i>	29
BAB IV HASIL DAN PEMBAHASAN	32
4.1 Hasil Sistem E-Voting	32

4.2	Analisis Performa Sistem E-Voting.....	34
BAB V PENUTUP		52
5.1	Kesimpulan	52
5.2	Saran	52
DAFTAR PUSTAKA.....		54
LAMPIRAN		57



DAFTAR TABEL

Tabel 1. Tabel Pemungutan Suara.....	23
Tabel 2. Tabel Perbandingan Percobaan Serangan Pada Sistem.....	35



DAFTAR GAMBAR

Gambar 2.1. Alur Sederhana Proses Enkripsi Dekripsi.....	10
Gambar 2.2. Struktur Umum Pendekatan Homomorfik E-Voting(Kho dkk.,.....	11
Gambar 2.3. Flowchart Algoritma Paillier	13
Gambar 3.1. Metode Penelitian	18
Gambar 3.2. Tahapan Implementasi.....	24
Gambar 3.3. DFD Level 0.....	24
Gambar 3.4. DFD Level 1.....	25
Gambar 3.5. Pembuatan Kunci.....	26
Gambar 3.6. Proses Enkripsi.....	27
Gambar 3.7. Proses Dekripsi.....	27
Gambar 3.8. Proses Homomorfik	28
Gambar 3.9. Contoh Enkripsi Dan Dekripsi Algoritma Paillier	28
Gambar 3.10. Kode Skenario Timing Attack E-Voting Tanpa Algoritma(1).....	29
Gambar 3.11. Kode Skenario Timing Attack E-Voting Tanpa Algoritma(2).....	30
Gambar 3.12. Kode Skenario Timing Attack E-Voting Tanpa Algoritma(3).....	30
Gambar 3.13. Kode Skenario Timing Attack Pada Website E-Voting	31
Gambar 4.1. Halaman Dashboard Admin	32
Gambar 4.2. Halaman List Voters.....	32
Gambar 4.3. Halaman Posisi Dan Nama Kandidat.....	33
Gambar 4.4. Halaman Kotak Suara.....	33
Gambar 4.5. Halaman Surat Suara Yang Sudah Dipilih.....	34
Gambar 4.6. Timing Attack Terhadap Sistem Evoting Tanpa Enkripsi.....	35
Gambar 4.7. Timing Attack Terhadap Sistem Evoting Dengan Enkripsi.....	35