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*

Skripsi

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

Oleh:

AGNES GABRIELLA MANIK

NIM 2001020043

Telah mengetahui dan disetujui oleh :

Pembimbing I,	**Pembimbing II,**
Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D.	Nurul Hayaty, S.T., M.Cs
NIDN. 0002048401	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

Ir. 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 kehadirat 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 meyediakan tenaga dan pikiran serta waktu untuk bimbingan ketika penyusunan skripsi.

7. Ibu Nurul Hayaty, S.T., M.Cs selaku pembimbing II yang meyediakan waktu, tenaga dan juga pikiran serta membimbing penyusunan skripsi.
8. Dosen penguji karena telah memberikan masukkan, 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

DAFTAR TABEL

DAFTAR GAMBAR