IMPLEMENTASI KRIPTOGRAFI HOMOMORPHIC MENGGUNAKAN ALGORTIMA PAILLIER CRYPTOSYSTEM PADA APLIKASI E-VOTING MOBILE

SKRIPSI

Oleh :

Fikki Arsyi Nur Fadlilah

202010225026

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS BHAYANGKARA JAKARTA RAYA

2024

LEMBAR PERSETUJUAN PEMBIMBING

Judul Proposal Tugas Akhir	:	Implementasi Kriptografi Homomorfik Menggunakan Algortima Paillier Cryptosystem Pada Aplikasi E-Voting Mobile
Nama Mahasiswa	:	Fikki Arsyi Nur Fadlilah
Nomor Pokok Mahasiswa	:	202010225026
Program Studi/Fakultas	:	Informatika / Ilmu Komputer

Jakarta, 05 Juli 2024

MENYETUJUI,

Pembimbing I	Pembimbing II
Asep Ramdhani Mahbub, S.kom., M.kom	**Dr. Robertus Suraji, S.S., M.A**
NIDN : 0329087703	NIDN : 0609127001

Ketua Program Studi

(Ahmad Fathurrozi, S.E., M.M.S.I.)

NIDN : 0327117402

LEMBAR PENGESAHAN

Judul Skripsi	:	Implementasi Kriptografi Homomorphic Menggunakan Algoritma Paillier Cryptosystem Pada Aplikasi E-voting Mobile
Nama Mahasiswa	:	Fikki Arsyi Nur Fadlilah
Nomor Pokok Mahasiswa	:	202010225026
Program Studi/Fakultas	:	Informatika/Ilmu Komputer
Tanggal Lulus Ujian Skripsi	:	27 Juni 2024

Jakarta, 05 Juli 2024

MENGESAHKAN,

Ketua Tim Penguji	:	Ahmad Fathurrozi, S.E., M.M.S.I. NIDN. 0327117402
Penguji I	:	Ajif Yunizar Pratama Yusuf, S.Si., M.Eng. NIDN. 0328068603
Penguji II	:	Asep Ramdhani Mahbub, S.Kom., M.Kom NIDN. 0329087703

MENGETAHUI,

Ketua Program Studi Informatika	Dekan Fakultas Ilmu Komputer
Ahmad Fathurrozi, S.E., M.M.S.I	Dr. Dra. Tyastuti Sri Lestari, M.M.
NIP. 2012486	NIP. 1408206

UNIVERSITAS BHAYANGKARA JAKARTA RAYA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA

LEMBAR PERNYATAAN BUKAN PLAGIASI

Yang bertanda tangan dibawah ini :

Nama	: Fikki arsyi Nur Fadlilah
NPM	: 202010225026
Program Studi	: Informatika
Fakultas	: Ilmu Komputer
Judul Tugas Akhir	: Implementasi Kriptografi Homomorfik Pada Aplikasi E-Voting Mobile Untuk Pemilihan Ketua RW: "Keamanan Dan Privasi Pemilih"

Dengan ini menyatakan bahwa hasil penulisan skripsi yang telah saya buat ini merupakan **hasil karya saya sendiri dan benar keasliannya**. Apabila dikemudian hari penulisan skripsi ini merupakan plagiat atau penjiplakan terhadap karya orang lain, maka saya bersedia mempertanggungjawabkan sekaligus bersedia menerima sanksi berdasarkan tata tertib di Universitas Bhayangkara Jakarta Raya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan dari pihak manapun.

Jakarta, 05 Juli 2024
Penulis

Fikki Arsyi Nur Fadlilah

ABSTRAK

Fikki Arsyi Nur Fadlilah. 202010225026. Implementasi Kriptografi Homomorphic Menggunakan Algoritma *Paillier Cryptosystem* Pada Aplikasi E-voting Mobile. Bekasi: Fakultas Ilmu Komputer. Universitas Bhayangkara Jakarta Raya. 2024.

Pemilihan ketua RW adalah salah satu aspek demokratis yang vital dalam mengatur lingkungan pemukiman. Namun, seringkali proses ini rentan terhadap kecurangan, intimidasi, dan pelanggaran privasi pemilih. Penelitian ini bertujuan untuk mengembangkan aplikasi e-voting mobile yang mengadopsi kriptografi homomorfik untuk meningkatkan keamanan dan privasi dalam proses pemilihan ketua RW. Metode yang digunakan adalah metode kuantitatif dengan menggunakan metode survei dan wawancara. Hasil penelitian menunjukkan bahwa aplikasi e-voting mobile yang mengadopsi kriptografi homomorfik dapat meningkatkan tingkat keamanan dan menjaga privasi dalam proses pemilihan ketua RW, meningkatkan kinerja dan efisiensi proses pemilihan, dan memperkuat keamanan dan integritas suara dalam proses pemilihan. Disarankan untuk mengembangkan aplikasi e-voting mobile yang mengadopsi kriptografi homomorfik untuk meningkatkan keamanan dan integritas suara dalam proses pemilihan.

Kata kunci: Implementasi, Kriptografi, Evoting, Mobile, Paillier Cryptosystem

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK

Sebagai sivitas akademik Universitas Bhayangkara Jakarta Raya, saya yang bertanda tangan di bawah ini :

Nama	: Fikki Arsyi Nur Fadlilah
NPM	: 202010225026
Program Studi	: Informatika
Fakultas	: Ilmu Komputer
Jenis Karya	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bhayangkara Jakarta Raya **Hak Bebas Royalti Non-Esklusif (*Non-Exclusive Royalty-Free Right*)**, atas karya ilmiah saya yang berjudul :

IMPLEMENTASI KRIPTOGRAFI HOMOMORFIK PADA APLIKASI E-VOTING MOBILE UNTUK PEMILIHAN KETUA RW: "KEAMANAN DAN PRIVASI PEMILIH"

beserta perangkat yang ada (bila diperlukan). Dengan hak bebas royalti non-ekslusif ini, Universitas Bhayangkara Jakarta Raya berhak menyimpan, mengalihmediakan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya dan mempublikasikannya di Internet atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik hak cipta.

Segala bentuk tuntutan hukum yang timbul atas pelanggaran hak cipta dalam karya ilmiah ini menjadi tanggung jawab saya pribadi

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal : 05 Juli 2024
Yang Menyatakan

Fikki Arsyi Nur Fadlilah

KATA PENGANTAR

Segala puji penulis panjatkan bagi Allah SWT yang telah memberikan rahmat dan hidayahnya sehingga saya dapat menyelesaikan proposal penelitian skripsi yang berjudul "Implementasi Kriptografi Homomorfik Menggunakan Paillier Cryptosystem Pada Aplikasi E-voting Mobile".

Penulisan proposal skripsi ini merupakan salah satu syarat untuk menyelesaikan tugas akhir program studi Informatika pada Fakultas Ilmu Komputer Universita Bhayangkara Jakarta Raya yang merupakan hasil dari upaya yang dilakukan selama beberapa waktu.

Dalam pembuatan proposal skripsi ini, penulis mendapatkan dukungan dari beberapa pihak untuk membantu dalam penelitian ini. Oleh karena itu penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Irjen Pol. (Purn) Dr.Drs. Bambang Karsosno, S.H., M.M. Selaku Rektor Universitas Bhayangkara Jakarta Raya
2. Ibu Dr.Dra Tyastuti Sri Lestari. M.M. Selaku Dekan Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Rya.
3. Bapak Ahmad Fathurrozi, S.E., MMSI. Selaku Ketua Program Studi Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
4. Bapak Asep Ramdhani Mahbub, S.kom., M.kom._selaku pembimbing 1 skripsi, dan Bapak Dr. Robertus Suraji, S.S, MA. Selaku pembimbing 2 yang telah memberikan arahan, bimbingan serta masukan yang sangat berharga sejak awal penelitian hingga penulisan skripsi ini. Bimbingan dan

pengajaran yang telah diberikan telah membantu penulis dalam memperoleh wawasan dan pemahaman yang lebih dalam terkait dengan topik penelitian.

5. Kepada keluarga penulis dan Ibu Apt. Neng Indy Maulida.S.Farm yang selalu memberikan doa, dukungan dan semangat dalam setiap langkah perjalanan penulisan skripsi ini. Terima kasih atas pengertian, kesabaran serta dukungan moril dan materil yang diberikan.
6. Kepada teman – teman penulis yang selalu memberikan semangat, dorongan, dan diskusi yang konstruktif dalam menjalani perjalanan penulisan skripsi ini. Terima kasih atas kerjasama, saran dan masukan yang berharga.
7. Kepada semua responden dan pihak yang telah berkenan meluangkan waktu serta memberikan data dan informasi dalam penelitian ini. Tanpa partisipasi dan kerjasama mereka, penelitian ini tidak akan terwujud.

Akhir kata, penulis menyadari bahwa skripsi ini tidak sempurna. Oleh karena itu, kritik, saran dan masukan yang membangun dari pembaca skripsi ini sangat penulis harapkan untuk menyempurnakan penelitian di masa depan. Semoga skripsi ini dapat memberikan manfaat dan kontribusi yang bermanfaat bagi pengembang ilmu. Semoga Allah SWT senantiasa memberikan rahmat dan hidayah-Nya kepada kita semua. Aamiin.

Bekasi, 05 Juli 2024
Penulis

Fikki Arsyi Nur Fadlilah

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR