

**IMPLEMENTASI KRIPTOGRAFI HOMOMORPHIC
MENGUNAKAN ALGORITMA 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 Algoritma Paillier
Cryptosystem Pada Aplikasi E-Voting Mobile

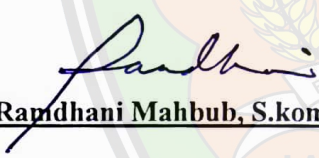
Nama Mahasiswa : Fikki Arsyi Nur Fadlilah
Nomor Pokok Mahasiswa : 202010225026
Program Studi/Fakultas : Informatika / Ilmu Komputer

Jakarta, 05 Juli 2024

MENYETUJUI,

Pembimbing I

Pembimbing II

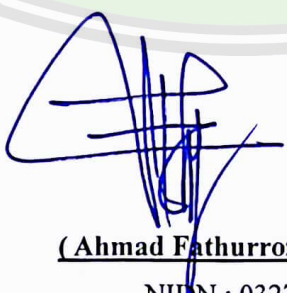

Asep Ramdhani Mahbub, S.kom., M.kom

NIDN : 0329087703


Dr. Robertus Suraji, S.S., M.A

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/Illmu 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
NIP. 2012486

Dr. Dra. Tyastuti Sri Lestari, M.M.
NIP. 1408206



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-Eksklusif (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-eksklusif 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 Universitas 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

LEMBAR PERSETUJUAN PEMBIMBING.....	i
LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN BUKAN PLAGIASI	iii
ABSTRAK.....	iv
ABSTRACT	v
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	ix
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
BAB I.....	1
PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	3
1.3 Batasan Masalah.....	4
1.4 Rumusan Masalah	4
1.5 Tujuan Penelitian.....	5

1.6	Manfaat Penelitian.....	5
1.7	Sistematika Penulisan.....	6
BAB II		8
TINJAUAN PUSTAKA		8
2.1	Penelitian Terdahulu.....	8
2.2	<i>E - Voting</i>	12
2.3	<i>Kriptografi</i>	13
2.3.1	<i>Sistem Kriptografi (Cryptosystem)</i>	14
2.4	<i>Enkripsi Homomorfik</i>	14
2.5	<i>Paillier Cryptosystem</i>	16
2.6	<i>Mobile Android</i>	19
2.7	<i>Pemilu (Pemilihan Umum)</i>	20
2.7.1	<i>Peraturan Pemilihan Ketua RW</i>	20
2.8	<i>Pengertian Firebase</i>	21
2.9	<i>Pengertian Aplikasi</i>	22
2.10	<i>Metode Waterfall</i>	22
2.10.1	<i>Keunggulan dan Kelemahan Metode Waterfall</i>	22
BAB III		24
METODOLOGI PENELITIAN		24
3.1	Tempat, Waktu dan Objek Penelitian	24

3.2	Kerangka Penelitian	25
3.3	Metode Pengumpulan Data	28
3.4	Analisis Sistem Berjalan	30
3.5	Permasalahan.....	32
3.6	Analisis Usulan Sistem.....	32
3.7	Analisis Kebutuhan Sistem	33
3.7.1	Kebutuhan Perangkat Keras (Hardware).....	34
3.7.2	Kebutuhan Perangkat Lunak (Software)	34
BAB IV		35
HASIL DAN PEMBAHASAN		35
4.1	Perancangan Sistem.....	35
4.2	Flowchart.....	35
4.2.1	Flowchart Panitia.....	36
4.2.1	Flowchart Kandidat.....	37
4.2.1	Flowchart Pemilih / Voter.....	38
4.3	UML (<i>Unified Modeling Language</i>)	39
4.3.1	Use Case Diagram.....	39
4.3.2	Activity Diagram.....	41
4.3.3	Sequence Diagram.....	49
4.3.4	Class Diagram	54

4.4	Perancangan Database	55
4.4	Perancangan Antarmuka.....	57
4.5	Implementasi Antarmuka.....	67
4.6	Implementasi Algoritma <i>Paillier Cryptosystem</i>	77
4.7	Pengujian Sistem	80
4.7.1	<i>Rencana Pengujian</i>	80
4.7.2	<i>Hasil Pengujian</i>	81
4.8	Hasil Pembahasan.....	82
BAB V		83
PENUTUP		83
5.1	Kesimpulan.....	83
5.2	Saran.....	83
DAFTAR PUSTAKA		84
LAMPIRAN		88
Lampiran 1		89
Lampiran 2		92
Lampiran 3		96

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu	8
Tabel 3. 1 Pertanyaan Wawancara	34
Tabel 3. 2 Jawaban Pihak Warga	34
Tabel 4. 1 Penjelasan Use Case Diagram Aplikasi Evoting	44
Tabel 4. 2 Candidates	60
Tabel 4. 3 Elections	60
Tabel 4. 4 User	61
Tabel 4. 5 Hasil Pengujian	85



DAFTAR GAMBAR

Gambar 2. 1	Diagram Implementasi Kriptografi	12
Gambar 2. 2	Jenis Enkripsi Homomorphic	13
Gambar 3. 1	Peta Lokasi Kantor RW 001	23
Gambar 3. 2	Kerangka Penelitian	30
Gambar 3. 3	Diagram alur Penelitian	32
Gambar 3. 4	Flowchart Analisis Sistem Berjalan	34
Gambar 3. 5	Diagram Analisis Usulan sistem	36
Gambar 4. 1	Flowchart Panitia	40
Gambar 4. 2	Flowchart Kandidat	41
Gambar 4. 3	Flowchart Pemilih / Voter	42
Gambar 4. 4	Use Case Diagram	43
Gambar 4. 5	Activity Diagram Login Kandidat dan Pemilih	45
Gambar 4. 6	Activity Diagram Login Panitia	46
Gambar 4. 7	Activity Diagram Kelola Data Kandidat Atau Pemilih	47
Gambar 4. 8	Activity Diagram Kelola Data Pemilihan	48
Gambar 4. 9	Activity Diagram Melakukan Pemilihan	49
Gambar 4. 10	Activity Diagram Melihat Hasil Pemilihan Sebelumnya	50
Gambar 4. 11	Activity Diagram Melihat Perhitungan Pemilihan	51
Gambar 4. 12	Activity Diagram Melihat Hasil Pemilihan	52
Gambar 4. 13	Sequence Login Panitia	53
Gambar 4. 14	Sequence Login Pemilih Dan Kandidat	54
Gambar 4. 15	Sequence Kelola Data Pemilih Dan Kandidat Oleh Panitia	55

Gambar 4. 16 Sequence Kelola Data Pemilihan Oleh Panitia	56
Gambar 4. 17 Sequence Melakukan Pemilihan Oleh Pemilih	57
Gambar 4. 18 Sequence Hasil Pemilihan Oleh Pemilih Dan Kandidat	58
Gambar 4. 19 Class Diagram Aplikasi E-Voting	59
Gambar 4. 20 Rancangan Halaman Register	62
Gambar 4. 21 Rancangan Halaman Login	63
Gambar 4. 22 Rancangan Data Diri Pemilih Dan Kandidat	64
Gambar 4. 23 Rancangan Halaman Utama Pemilih	65
Gambar 4. 24 Rancangan Halaman Utama Kandidat	66
Gambar 4. 25 Rancangan Halaman Utama Panitia	67
Gambar 4. 26 Rancangan Halaman Buat Pemilihan	68
Gambar 4. 27 Rancangan Halaman Vote	69
Gambar 4. 28 Rancangan Halaman Hasil Pemilihan	70
Gambar 4. 29 Hasil Halaman Registrasi	71
Gambar 4. 30 Hasil Halaman Login	72
Gambar 4. 31 Hasil Halaman Data Diri	73
Gambar 4. 32 Hasil Halaman Utama Pemilih	74
Gambar 4. 33 Hasil Halaman Pemilihan	75
Gambar 4. 34 Hasil HalamanVote Kandidat	76
Gambar 4. 35 Hasil Dari Pemilihan	77
Gambar 4. 36 Hasil Halaman Utama Kandidat	78
Gambar 4. 37 Hasil Halaman Utama Panitia	79
Gambar 4. 38 Hasil Halaman Create elections	80

Gambar 4. 39 <i>Encryption Method</i>	81
Gambar 4. 40 <i>Calculate Election Result</i>	82
Gambar 4. 38 Hasil Enkripsi Di <i>Database</i>	83
Gambar 4. 42 Hasil Pemilihan	83

