PENINGKATAN KECEPATAN ENKRIPSI *PAILLIER HOMOMORPHIC CRYPTOSYSTEM* DENGAN *CHINESE REMAINDER THEOREM* PADA SISTEM *E-VOTING*

Diajukan Sebagai Syarat untuk Menyelesaikan
Pendidikan Program Strata-1 pada
Jurusan Teknik Informatika

Oleh:

Billy Dipta Yulio

09021281520097

JURUSAN TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2019

LEMBAR PENGESAHAN TUGAS AKHIR

PENINGKATAN KECEPATAN ENKRIPSI *PAILLIER HOMOMORPHIC CRYPTOSYSTEM* DENGAN *CHINESE REMAINDER THEOREM* PADA SISTEM *E-VOTING*

Oleh :

BILLY DIPTA YULIO

NIM : 09021281520097

Indralaya, 23 Desember 2019

Mengetahui,

Pembimbing I,

Drs. Megah Mulya, M.T

NIP. 19660220006041001

Pembimbing II,

Osvari Arsalan, M.T

NIP. 198806282018031001

Mengetahui,

Ketua Jurusan Teknik Informatika,

Rifkie Primartha, M.T

NIP. 197706012009121004

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari **Rabu** tanggal **18 desember 2019** telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Billy Dipta Yulio
NIM : 09021281520097
Judul : PENINGKATAN KECEPATAN ENKRIPSI *PAILLIER HOMOMORPHIC CRYPTOSYSTEM* DENGAN *CHINESE REMAINDER THEOREM* PADA SISTEM *E-VOTING*

1. Pembimbing I

Drs. Megah Mulya, M.T
NIP. 19660220006041001 .....

2. Pembimbing II

Osvari Arsalan, M.T
NIP. 198806282018031001 .....

3. Penguji I

M. Fachrurrozi, M.T
NIP 198005222008121002 .....

4 Penguji II

Kanda Januar Miraswan, M.T
NIPUS. 1671080901900006 .....

Mengetahui,
Ketua Jurusan Teknik Informatika

Rifkie Primartha M.T.
NIP 197706012009121004

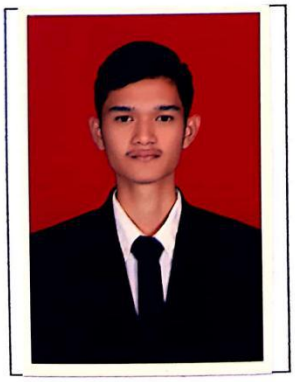
HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Billy Dipta Yulio
NIM	: 09021281520097
Program Studi	: Teknik Informatika
Judul Skripsi	: PENINGKATAN KECEPATAN ENKRIPSI PAILLIER HOMOMORPHIC CRYPTOSYSTEM DENGAN CHINESE REMAINDER THEOREM PADA SISTEM E-VOTING
Hasil Pengecekan Software *iThenticate/Turnitin*	: 10%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.



Palembang, 23 Desember 2019

Billy Dipta Yulio
NIM. 09021281520097

Motto:

- *Braccas meas vescimini*
- *Fas est ab hoste doceri*

Kupersembahkan karya tulis ini kepada :

- *Orang tuaku tersayang*
- *Keluarga besarku*
- *Sahabat dan teman seperjuanganku*
- *Fakultas Ilmu Komputer Universitas Sriwijaya*

IMPROVEMENT OF HOMOMORPHIC CRYPTOSYSTEM PAILLIER ENCRYPTION SPEED WITH CHINESE REMAINDER THEOREM IN E-VOTING SYSTEM

By:
Billy Dipta Yulio
09021281520097

ABSTRACT

Encryption becomes the last shield to secure a message. Research on encryption has become a developing field. In general, the encryption stage is divided into three: key generation, encryption, and decryption. Many kinds of encryption methods. One of them is encryption which has homomorphic properties. Homomorphic nature is a trait that can perform operations on messages that are still encrypted. There are two types of homomorphic properties. Namely additive and multiplicative homomorphisms. Paillier Encryption is encryption with additive homomorphism properties. Paillier encryption also has semantic security properties. With these two characteristics, Paillier encryption has the potential to secure messages on e-voting systems. However, the speed at the encryption stage is slow for Paillier's method. Chinese remainder theorem can simplify the calculation of the encryption stage of the Paillier algorithm.

Keywords: *Encryption, homomorphic, e-voting, Paillier, Chinese remainder theorem*

Inderalaya, December 19, 2019

Supervisor I,

Drs. Megah Mulya, M.T
NIP. 19660220006041001

Supervisor II,

Osvari Arsalan, M.T
NIP. 198806282018031001

Approved,
Chairman of Informatic Engineering Department

Rifkie Primartha, M.T
NIP. 197706012009121004

vi

PENINGKATAN KECEPATAN ENKRIPSI *PAILLIER HOMOMORPHIC CRYPTOSYSTEM* DENGAN *CHINESE REMAINDER THEOREM* PADA SISTEM *E-VOTING*

By:
Billy Dipta Yulio
09021281520097

ABSTRAK

Enkripsi menjadi tameng terakhir dalam mengamankan suatu pesan. Penelitian tentang enkripsi telah menjadi bidang yang berkembang. Secara umum, tahap enkripsi dibagi menjadi tiga: pembangkitan kunci, enkripsi dan dekripsi. Banyak macam-macam metode enkripsi. Salah satunya adalah enkripsi yang memiliki sifat homomorfik. Sifat homomorfik adalah sifat dimana dapat melakukan operasi pada pesan yang masih terenkripsi. Ada dua jenis sifat homomorfik. Yaitu homomorfik *additive* dan *multiplicative*. Enkripsi Paillier merupakan enkripsi dengan sifat *additive homomorphism*. Enkripsi Paillier juga mempunyai sifat *semantic security*. Dengan dua sifat ini, enkripsi Paillier berpotensi dalam mengamankan pesan pada sistem *e-voting*. Namun, kecepatan pada tahap enkripsi terbilang lambat untuk metode Paillier. Chinese remainder theorem dapat menyederhanakan perhitungan dari tahap enkripsi pada algoritma Paillier.

Kata Kunci: *Enkripsi, homomorfik, e-voting, Paillier, Chinese remainder theorem*

Inderalaya, 19 Desember 2019

Pembimbing I,	Pembimbing II,
Drs. Megah Mulya, M.T	Osvari Arsalan, M.T
NIP. 19660220006041001	NIP. 198806282018031001

Mengetahui,
Ketua Jurusan Teknik Informatika

Rifkie Primartha, M.T
NIP. 197706012009121004

vii

KATA PENGANTAR

Puji syukur kepada Allah SWT atas berkat dan rahmat-Nya yang telah diberikan kepada Penulis sehingga dapat menyelesaikan Tugas Akhir ini dengan baik. Tugas Akhir ini disusun untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Dalam menyelesaikan Tugas Akhir ini banyak pihak yang telah memberikan bantuan dan dukungan baik secara langsung maupun secara tidak langsung. Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih kepada pihak-pihak yang telah membantu penulis dalam menyelesaikan Tugas Akhir ini, yaitu kepada:

1. Orang tuaku, serta seluruh saudara-saudariku yang selalu mendoakan serta memberikan dukungan baik moril maupun materil.
2. Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Rifkie Primartha, S.T., M.T. selaku Ketua Jurusan Teknik Informatika sekaligus sebagai pembimbing Tugas Akhir yang telah membimbing, mengarahkan dan memberikan motivasi penulis dalam proses perkuliahan dan pengerjaan Tugas Akhir.
4. Bapak Drs. Megah Mulya, M.T dan bapak Osvari Arsalan, M.T selaku dosen pembimbing akademik, yang telah membimbing, mengarahkan, dan memberikan motivasi penulis dalam proses perkuliahan.
5. Bapak M. Fachrurrozi, M.T, selaku dosen penguji I, yang telah memberikan masukkan dan dorongan dalam proses pengerjaan Tugas Akhir.
6. Bapak Kanda Januar Miraswan, M.T selaku dosen penguji II, yang telah memberikan masukkan dan dorongan dalam proses pengerjaan Tugas Akhir.
7. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Kak Ricy Selaku pahlawan mencari kebenaran di hari sidang.
9. Silampari, atas minuman penyemangatnya.
10. Rahma Yunita, sebagai alarm super yang setiap hari selalu mengingatkan untuk mengerjakan laporan.
11. Anak GP, yang menyatakan 5 tahun bisa. Silahkan kalian sendiri yang 5 tahun. Saya cabut.

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan disebabkan keterbatasan pengetahuan dan pengalaman, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk kemajuan penelitian selanjutnya.

Akhir kata semoga Tugas Akhir ini dapat berguna dan bermanfaat bagi kita semua.

Indralaya, Desember 2019

Billy Dipta Yulio

DAFTAR ISI

Halaman

JUDUL..... i
LEMBAR PENGESAHAN TUGAS AKHIR.....ii
TANDA LULUS UJIAN SIDANG TUGAS AKHIR..... iii
HALAMAN PERNYATAAN..... iv
ABSTRACT..... vi
ABSTRAK..... vii
KATA PENGANTAR..... viii
DAFTAR ISI..... x
DAFTAR TABEL.....xiii
DAFTAR GAMBAR.....xv
BAB I PENDAHULUAN.....I-1
1.1 Pendahuluan..... I-1
1.2 Latar Belakang Masalah.....I-1
1.3 Rumusan masalah.....I-3
1.4 Tujuan Penelitian.....I-4
1.5 Manfaat Penelitian.....I-4
1.6 Batasan Masalah.....I-4
1.7 Sistematika Penulisan.....I-5
1.8 Kesimpulan.....I-6
BAB II KAJIAN LITERATUR.....II-1
2.1 Pendahuluan.....II-1
2.2 Kriptografi.....II-1
2.3 Kriptosistem Paillier..... II-2
2.4 Sifat Homomorfik..... II-5
2.5 Chinese Remainder Theorem.....II-6
2.6 E-Voting.....II-8

2.7 Algoritma Paillier-CRT.....II-10

2.7.1 Pembangkitan Kunci Paillier-CRT..... II-10

2.7.2 Enkripsi Paillier-CRT..... II-10

2.7.3 Dekripsi Paillier-CRT..... II-11

2.8 Rational Unified Process.....II-12

2.9 Penelitian yang relevan..... II-13

2.9.1 Anggriane, Nasution dan Azmi (2017) - Advanced e-voting system using Paillier homomorphic encryption algorithm.....II-13

2.9.3 Desi Wulansari, Much Aziz Muslim dan Endang Sugiharti (2016) - Implementation of RSA Algorithm with Chinese Remainder Theorem for Modulus N 1024 Bit and 4096 Bit.....II-15

2.9.2 Dini Amalia (2017) - PENGAMANAN SMS PADA PERANGKAT ANDROID DENGAN MENGGUNAKAN RSA-CRT.....II-16

2.10 Kesimpulan..... II-17

BAB III METODOLOGI PENELITIAN.....III-1

3.1 Pendahuluan.....III-1

3.2 Pengumpulan Data.....III-1

3.2.1 Jenis dan Sumber Data.....III-1

3.2.2 Metode Pengumpulan Data.....III-1

3.3 Tahapan Penelitian.....III-2

3.3.1 Menetapkan Kerangka Kerja / Framework.....III-2

3.3.2 Menetapkan Kriteria Pengujian..... III-4

3.3.3 Menetapkan Format Data Pengujian..... III-4

3.3.4 Menentukan Alat yang Digunakan dalam Pelaksanaan PenelitianIII-5

3.3.5 Melakukan Pengujian Penelitian..... III-6

3.3.6 Melakukan Analisa Hasil Pengujian dan Membuat KesimpulanIII-6

3.4 Metode Pengembangan Perangkat Lunak..... III-7

3.4.1 Fase Insepsi.....III-7

3.4.2 Fase Elaborasi.....III-8

3.4.3 Fase Konstruksi..... III-8

3.4.4 Fase Transisi..... III-9

3.5 Manajemen Proyek Perangkat Lunak.....III-9
BAB IV PENGEMBANGAN PERANGKAT LUNAK..... IV-1
4.1 Pendahuluan..... IV-1
4.2 Fase Insepsi..... IV-1
4.2.1 Pemodelan Bisnis..... IV-2
4.2.2 Kebutuhan Sistem.....IV-2
4.2.3 Analisis dan Desain..... IV-5
4.3 Fase Elaborasi.....IV-17
4.3.1 Pemodelan Bisnis..... IV-18
4.3.2 Kebutuhan Sistem.....IV-20
4.3.3 Diagram Alur.....IV-21
4.4 Fase Konstruksi..... IV-24
4.4.1 Kebutuhan Sistem.....IV-24
4.4.2 Diagram Kelas..... IV-24
4.4.3 Implementasi..... IV-26
4.5 Fase Transisi.....IV-29
4.5.1 Pemodelan Bisnis..... IV-29
4.5.2 Kebutuhan Sistem.....IV-29
4.5.3 Rencana Pengujian..... IV-30
4.6 Kesimpulan.....IV-36
BAB V HASIL DAN ANALISIS PENELITIAN.....V-1
5.1 Pendahuluan.....V-1
5.2 Percobaan Penelitian.....V-1
5.3 Hasil Enkripsi Paillier dan Paillier-CRT..... V-3
5.4 Hasil Perhitungan Waktu Komputasi Enkripsi Paillier dan Paillier-CRT V-9
5.5 Analisa Penelitian..... V-14
5.6 Kesimpulan..... V-22
BAB VI KESIMPULAN DAN SARAN..... VI-1
6.1 Pendahuluan..... VI-1

6.2 Kesimpulan..... VI-1
6.3 Saran..... VI-2
DAFTAR PUSTAKA..... xvii

DAFTAR TABEL

Halaman

Tabel II- 1. hasil pengujian dekripsi dengan plaintext berbeda..... II-14
Tabel II- 2. hasil pengujian homomorfik..... II-14
Tabel II- 3. Hasil pengujian dekripsi RSA dan RSA-CRT II-15
Tabel II- 4. Hasil pengujian waktu dekripsi dengan kunci 1024 bit..... II-16
Tabel II- 5. Hasil pengujian waktu dekripsi dengan kunci 4096 bit II-16
Tabel III-1. Rancangan Tabel Hasil Pengujian Kecepatan Enkripsi III-4
Tabel III-2. Rancangan tabel hasil analisa peningkatan waktu enkripsi..... III-7
Tabel III-3. Work Breakdown Structure (WBS)..... III-10
Tabel IV–1. Kebutuhan Fungsional IV-4
Tabel IV–2. Kebutuhan Non Fungsional..... IV-4
Tabel IV-3. Contoh Hasil Enkripsi Paillier dan Paillier-CRT IV-7
Tabel IV-4. Contoh Hasil Dekripsi Homomorfik dengan 1000 suara..... IV-7
Tabel IV-5. Contoh Hasil Perhitungan Lama Komputasi..... IV-8
Tabel IV-6. Definisi Aktor..... IV-9
Tabel IV-7. Definisi Use Case IV-10
Tabel IV-8. Skenario Use Case Melakukan proses enkripsi Paillier dan Paillier-CRT..... IV-11
Tabel IV-9. Skenario Use Case Melakukan Perhitungan waktu lama komputasi enkripsi..... IV-12
Tabel IV-10. Skenario Use Case Melakukan dekripsi pada data homomorfik IV-13
Tabel IV–11. Tabel Implementasi Kelas..... IV-26
Tabel IV-12. Rencana Pengujian Use Case Melakukan proses enkripsi Paillier dan Paillier-CRT..... IV-30
Tabel IV-13. Rencana Pengujian Use Case Melakukan Perhitungan waktu lama komputasi enkripsi..... IV-31
Tabel IV-14. Rencana Pengujian Use Case Melakukan dekripsi pada data homomorfik..... IV-31
Tabel IV-15. Pengujian Use Case Melakukan proses enkripsi Paillier dan Paillier-CRT IV-33
Tabel IV-16. Pengujian Use Case Melakukan Perhitungan waktu lama komputasi enkripsi..... IV-34

Tabel IV-17. Pengujian Use Case Melakukan dekripsi pada data homomorfik IV-35
Tabel V-1. Hasil Suara dari Pemilih V-2
Tabel V-2. Hasil enkripsi Paillier dan Paillier-CRT kunci 64 bit V-3
Tabel V-3. Hasil enkripsi Paillier dan Paillier-CRT kunci 256 bit V-5
Tabel V-4. Hasil Enkripsi Paillier dan Paillier-CRT kunci 1024 bit..... V-6
Tabel V-5. Hasil Enkripsi Paillier dan Paillier-CRT Kunci 2048 bit..... V-7
Tabel V-6. Hasil Perhitungan Waktu Komputasi Enkripsi Paillier dan Paillier-CRT Kunci 64 bit..... V-9
Tabel V-7. Hasil Perhitungan Waktu Komputasi Enkripsi Paillier dan Paillier-CRT Kunci 256 bit V-10
Tabel V-8. Hasil Perhitungan Waktu Komputasi Enkripsi Paillier dan Paillier-CRT kunci 1024 bit V-11
Tabel V-9. Hasil Perhitungan Waktu Komputasi Enkripsi Paillier dan Paillier-CRT Kunci 2048 bit V-12
Tabel V-10. Selisih Waktu Komputasi Enkripsi Paillier dan Paillier-CRT Kunci 64 bit V-13
Tabel V-11. Selisih Waktu Komputasi Enkripsi Paillier dan Paillier-CRT Kunci 256 bit V-14
Tabel V-12. Selisih Waktu Komputasi Enkripsi Paillier dan Paillier-CRT kunci 1024 bit..... V-15
Tabel V-13. Selisih waktu komputasi enkripsi Paillier dan Paillier-CRT kunci 2048 bit V-16
Tabel V-14. Hasil Analisa Peningkatan Kecepatan Enkripsi Paillier untuk Tiap Kunci 64 bit, 256 bit, 1024 bit dan 2048 bit..... V-18

DAFTAR GAMBAR

Halaman

Gambar II-1. Desain sistem e-voting..... II-9
Gambar II-2. Arsitektur RUP (Kruchten, 2004)..... II-12
Gambar II-3. Hasil pengujian waktu enkripsi dan dekripsi..... II-14
Gambar II-4. Hasil perbandingan waktu dekripsi RSA dan RSA-CRT..... II-17
Gambar III-1. Diagram Tahap Penelitian..... III-2
Gambar III-2. Tahapan Pengujian Kecepatan Enkripsi III-6
Gambar III-3. Gantt Chart Penjadwalan Penelitian Tahap Menentukan Ruang Lingkup dan Unit Penelitian..... III-14
Gambar III-4. Gantt Chart Penjadwalan Penelitian Tahap Menentukan Dasar Teori yang Berkaitan dengan Penelitian..... III-14
Gambar III-5. Gantt Chart Penjadwalan Penelitian Tahap Menentukan Kriteria Pengujian..... III-15
Gambar III-6. Gantt Chart Penjadwalan Penelitian Tahap Menentukan Alat yang Digunakan Untuk Pelaksanaan Penelitian pada Fase Insepsi..... III-15
Gambar III-7. Gantt Chart Penjadwalan Penelitian Tahap Menentukan Alat yang Digunakan Untuk Pelaksanaan Penelitian pada Fase Elaborasi..... III-16
Gambar III-8. Gantt Chart Penjadwalan Penelitian Tahap Menentukan Alat yang Digunakan Untuk Pelaksanaan Penelitian pada Fase Konstruksi..... III-16
Gambar III-9. Gantt Chart Penjadwalan Penelitian Tahap Menentukan Alat yang Digunakan Untuk Pelaksanaan Penelitian pada Fase Transisi..... III-17
Gambar III-10. Gantt Chart Penjadwalan Penelitian Tahap Melakukan Pengujian Penelitian..... III-17
Gambar III-11. Gantt Chart Penjadwalan Penelitian Tahap Melakukan Analisa Hasil Pengujian dan Pembuatan Kesimpulan..... III-18
Gambar IV-1. Diagram Use Case Perangkat Lunak..... IV-9
Gambar IV-2 Melakukan Dekripsi pada Data Homomorfik IV-15
Gambar IV-3 Melakukan Perhitungan Waktu Lama Komputasi Enkripsi..... IV-16
Gambar IV-4 Melakukan Proses Enkripsi Paillier dan Paillier-CRT..... IV-17
Gambar IV-5 Rancangan Antarmuka Perangkat Lunak Utama..... IV-19
Gambar IV-6 Rancangan Antarmuka Perangkat Lunak Enkripsi..... IV-20
Gambar IV-7 Sequence Diagram Enkripsi..... IV-22
Gambar IV-8 Sequence Diagram Lama Komputasi..... IV-23

Gambar IV-9 Sequence Diagram Dekripsi Homomorfik.....IV-23
Gambar IV-10 Class Diagram IV-25
Gambar IV-11 Antarmuka Halaman Utama..... IV-28
Gambar IV-12 Antarmuka Halaman Enkripsi.....IV-28
Gambar V-1. Peningkatan Kecepatan Enkripsi dengan Kunci 64 bit dan 256 bit V-18
Gambar V-2 Peningkatan Kecepatan Enkripsi dengan Kunci 1024 bit dan 2048 bit V-19

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab ini akan dibahas latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian serta batasan masalah yang menjadi gambaran umum mengenai penelitian yang akan dilakukan.

Pendahuluan dimulai dengan penjelasan mengenai masalah dalam enkripsi pada enkripsi homomorfik. Penelitian yang berkaitan dengan enkripsi homomorfik yang digunakan disertakan dalam latar belakang dari penelitian ini.

1.2 Latar Belakang Masalah

Belakangan ini, mayoritas perusahaan-perusahaan berfikir untuk melakukan *outsource* pada infrastruktur IT pada pihak ketiga untuk mengurangi penyimpanan data dan biaya manajemen, dan untuk mendapatkan keuntungan yang ditawarkan oleh pihak ketiga(Beni-hssane, 2016). Namun, menyangkut data perusahaan yang sensitif dan rahasia menjadi halangan utama untuk memakai cara outsourcing data. Untuk mengamankan data yang rahasia, data bisa di enkripsi sebelum dikirimkan ke pihak ketiga menggunakan skema enkripsi yang efisien. Namun, untuk memberikan pihak ketiga akses manipulasi data, data ini harus didekripsi. Pada tahap ini bisa dikategorikan sebagai pelanggaran kerahasiaan karena pihak ketiga dapat melihat data sensitif dari perusahaan. Dari situlah, peneliti membuat sebuah teknik yang disebut dengan enkripsi homomorfik.

Teknik enkripsi homomorfik adalah bentuk enkripsi yang memperbolehkan komputasi dengan tipe spesifik seperti pertambahan dan perkalian pada data yang terenkripsi dan menghasilkan data terenkripsi(Beni-hssane, 2016). Hasil dekripsi dari operasi akan sama dengan nilai operasi yang langsung dilakukan pada plaintext. Kemampuan untuk melakukan komputasi pada *chipertext* tanpa mengetahui sedikitpun informasi dari plaintext membuat teknik ini berguna untuk berbagai macam protokol yang sangat menjaga kerahasiaan.

Salah satu sistem yang berpotensi besar menggunakan enkripsi homomorfik adalah sistem *e-voting*. Karena sistem voting secara manual memakan waktu, tidak praktis dan membutuhkan biaya yang tidak sedikit(Sharma, 2016), sistem *e-voting* cenderung bisa mengatasi semua keterbatasan ini. Beberapa skema enkripsi homomorfik yang dapat dipakai antara lain: RSA, ElGamal, Paillier dll. Sayangnya, skema enkripsi ini hanya mendukung operasi homomorfik yang terbatas. Skema enkripsi RSA dan ElGamal mendukung *multiplicative homomorphism*. Sementara Paillier mendukung *additive homomorphism*(Beni-hssane, 2016). Dengan menggunakan sifat *additive homomorphism* pada enkripsi Paillier, kita bisa melakukan operasi pertambahan vote dalam bentuk data terenkripsi. Penelitian yang menggunakan kriptosistem Paillier pada sistem *e-voting* dilakukan oleh Shifa Manaruliesya Anggriane, Surya Michrandi Nasution dan Fairuz Azmi(2017). Kriptosistem Paillier dapat diimplementasikan dengan baik pada sistem *e-voting* yang mereka buat. Namun muncul kelemahan, yaitu proses enkripsi yang lama. Hal ini cukup bermasalah,

dikarenakan proses enkripsi merupakan proses yang paling sering dilakukan pada sistem ini.

Algoritma Paillier memiliki 3 tahap, yaitu pembangkitan kunci, enkripsi dan dekripsi. Permasalahan dalam menghitung nilai residu *n*th dipercaya menjadi kekuatan Paillier dari segi keamanan(Yi, Paulet and Bertino, 2014). Di sisi lain, semakin kompleks nilai *n*, semakin lama proses enkripsi. *Chinese remainder theorem* (CRT) adalah suatu operasi untuk membagi operasi pemangkatan modular yang besar menjadi dua operasi pemangkatan yang lebih kecil(Amalia, 2017). Penggunaan CRT dilakukan oleh Desi Wulansari(2016) dan Dini Amalia(2017) pada algoritma RSA. Hasil akhir didapatkan bahwa RSA yang menggunakan CRT 3 kali lebih cepat dibandingkan RSA biasa.

Berdasarkan uraian latar belakang di atas, dapat diambil kesimpulan bahwa penelitian ini akan membahas tentang meningkatkan kecepatan enkripsi *Paillier homomorphic cryptosystem* dengan menggunakan *Chinese remainder theorem* pada sistem *e-voting.*

1.3 Rumusan masalah

Dikarenakan pada teknik homomorfik, tahap enkripsi merupakan tahap yang paling banyak melakukan komputasi, maka didapatkan rumusan permasalahan pada penelitian ini yaitu seberapa besar peningkatan enkripsi *Paillier homomorphic cryptosystem* menggunakan *Chinese remainder theorem* .

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengembangkan perangkat lunak enkripsi pesan sistem *e-voting*
2. Mengetahui kecepatan enkripsi Paillier
3. Mengetahui kecepatan enkripsi Paillier-CRT
4. Membandingkan kecepatan enkripsi Paillier dan Paillier-CRT

1.5 Manfaat Penelitian

Manfaat yang dapat diperoleh dari penelitian ini adalah hasil penelitian dapat digunakan untuk pengamanan pesan pada sistem *e-voting*.

1.6 Batasan Masalah

Batasan masalah dalam penelitian ini, yaitu sebagai berikut:

1. Pesan yang dienkripsi berupa nilai integer 1 dan 0.
2. Perangkat lunak menggunakan *stand alone*.
3. Tolak ukur pengujian atau pembanding adalah kecepatan pada tahap enkripsi.
4. Kandidat yang dapat dipilih berjumlah minimal tiga orang.

1.7 Sistematika Penulisan

Sistematika penulisan pada penelitian ini adalah sebagai berikut:

BAB I. PENDAHULUAN

Pada bab ini dijelaskan mengenai latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini akan dibahas dasar-dasar teori yang digunakan dalam penelitian, seperti tentang kriptografi, kriptosistem Paillier, sifat homomorfik, CRT, dan *e-voting*. Pada akhir bab akan disertakan penelitian-penelitian lain yang relevan dengan penelitian ini.

BAB III. METODOLOGI PENELITIAN

Pada bab ini dijelaskan mengenai tahapan yang akan dilaksanakan pada penelitian. Setiap rencana tahapan penelitian dideskripsikan dengan detail dengan mengacu pada suatu kerangka kerja. Pada akhir bab, berisi perancangan manajemen proyek pada pelaksanaan penelitian.

1.8 Kesimpulan

Enkripsi Paillier adalah enkripsi yang memiliki sifat dapat melakukan komputasi pertambahan dalam bentuk *chipertext*. Terdapat perhitungan yang kompleks pada saat enkripsi. Chinese remainder theorem dapat menyederhanakan perhitungan pada enkripsi yang diharapkan akan mempercepat proses enkripsi.

Berdasarkan uraian, pada penelitian ini akan dilakukan optimasi *Paillier homomorphic cryptosystem* dengan *Chinese remainder theorem* pada sistem *e-voting* dengan batasan masalah yang telah ditentukan.

DAFTAR PUSTAKA

Amalia, D. (2017) 'PENGAMANAN SMS PADA PERANGKAT ANDROID DENGAN MENGGUNAKAN ALGORITMA RSA-CRT'.

Anggriane, S. M., Nasution, S. M. and Azmi, F. (2017) 'Advanced e-voting system using Paillier homomorphic encryption algorithm', *2016 International Conference on Informatics and Computing, ICIC 2016*, (Icic), pp. 338–342. doi: 10.1109/IAC.2016.7905741.

Beni-hssane, A. (2016) 'Can Hybrid Homomorphic Encryption Schemes Be Practical ?', pp. 1–5.

Gentry, C. (2009) 'a Fully Homomorphic Encryption Scheme', *PhD Thesis*, (September), pp. 1–209. doi: 10.1145/1536414.1536440.

Harerimana, R., Tan, S. Y. and Yau, W. C. (2017) 'A Java implementation of paillier homomorphic encryption scheme', *2017 5th International Conference on Information and Communication Technology, ICoIC7 2017*, 0(c). doi: 10.1109/ICoICT.2017.8074646.

Mathur, H. and Alam, P. Z. (2015) 'Analysis in Symmetric and Asymmetric Cryptology Algorithm', *International Journal of Elmerging Trends and Technology in Computer Science*, 4(1), pp. 4–6.

Morris, L. (2013) 'Analysis of Partially and Fully Homomorphic Encryption Partially Homomorphic Cryp-'.

Ngo, C. (2014) ‘Secure Voting System Using Paillier Homomorphic Encryption’.

Sakurai, K. and Takagi, T. (2002) ‘On the Security of a Modified Paillier Public-Key Primitive’, pp. 436–448. doi: 10.1007/3-540-45450-0_33.

Samad, S., Haq, A. and Khan, S. A. (2015) ‘Orientation Invariant Object Recognitions Using Geometric Moments Invariants and Color Histograms’, 7(2), pp. 101–108.

Sharma, T. (2016) ‘E-Voting using Homomorphic Encryption Scheme’, 141(13), pp. 14–16.

Sridokmai, T. and Prakancharoen, S. (2015) ‘The homomorphic other property of Paillier cryptosystem’, *Proceedings 2015 International Conference on Science and Technology, TICST 2015*, pp. 356–359. doi: 10.1109/TICST.2015.7369385.

Suwandi, R., Nasution, S. M. and Azmi, F. (2016) ‘Okamoto-Uchiyama Homomorphic Encryption Algorithm Implementation in E-Voting System’, (Icic).

Wulansari, D. (2016) ‘Implementation of RSA Algorithm with Chinese Remainder Theorem for Modulus N 1024 Bit and 4096 Bit’, (10), pp. 186–194.

Yi, X., Paulet, R. and Bertino, E. (2014) ‘Homomorphic Encryption and Applications’, pp. 27–47. doi: 10.1007/978-3-319-12229-8.