IMPLEMENTASI KRIPTOGRAFI KURVA ELIPTIK DAN STEGANOGRAFI LEAST SIGNIFICANT BIT UNTUK PENYIMPANAN IDENTITAS

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom.)

Christofer Derian Budianto

14110110019

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK DAN INFORMATIKA

UNIVERSITAS MULTIMEDIA NUSANTARA

TANGERANG

2018

LEMBAR PENGESAHAN SKRIPSI

IMPLEMENTASI KRIPTOGRAFI KURVA ELIPTIK DAN STEGANOGRAFI LEAST SIGNIFICANT BIT UNTUK PENYIMPANAN IDENTITAS

Oleh

Nama	: Christofer Derian Budianto
NIM	: 14110110019
Fakultas	: Teknik dan Informatika
Program Studi	: Informatika

Tangerang, 9 Mei 2018

Ketua Sidang	Dosen Penguji
Ni Made Satvika Iswari, S.T., M.T.	Dennis Gunawan, S.Kom., M.Sc.
Dosen Pembimbing I	Dosen Pembimbing II
Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, CEH	Seng Hansun, S.Si., M.Cs.

Mengetahui,
Ketua Program Studi
Informatika

Seng Hansun, S.Si., M.Cs.

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya,

Nama : Christofer Derian Budianto

NIM : 14110110019

Fakultas : Teknik dan Informatika

Program Studi : Informatika

menyatakan bahwa skripsi yang berjudul "**IMPLEMENTASI KRIPTOGRAFI KURVA ELIPTIK DAN STEGANOGRAFI LEAST SIGNIFICANT BIT UNTUK PENYIMPANAN IDENTITAS"** ini adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan / penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah Skripsi yang telah saya tempuh.

Tangerang, 9 Mei 2018

(Christofer Derian Budianto)

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Multimedia Nusantara, saya yang bertanda tangan di bawah ini:

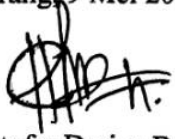
Nama : Christofer Derian Budianto
NIM : 14110110019
Program Studi : Informatika
Fakultas : Teknik dan Informatika
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui dan memberikan izin kepada **Universitas Multimedia Nusantara** hak Bebas Royalti Non-eksklusif *(Non-exclusive Royalti-Free Right)* atas karya ilmiah saya yang berjudul: **Implementasi Kriptografi Kurva Eliptik dan Steganografi Least Significant Bit untuk Penyimpanan Identitas** beserta perangkat yang diperlukan.

Dampak Hak Bebas Royalti Non-eksklusif ini, pihak Universitas Multimedia Nusantara Berhak menyimpan, mengalihmedia atau *format*-kan, mengelola dalam bentuk pangkalan data *(database)*, merawat, dan mendistribusi dan menampilkan atau mempublikasikan karya ilmiah saya di internet atau media ain untuk kepentingan akademis, tanpa perlu meminta izin dari saya maupun memberikan royalti kepada saya, selama tetap mencantumkan nama saya sebagai penulis karya ilmiah tersebut.

Demikian pernyataan ini saya buat dengan sebenarnya untuk dipergunakan sebagaimana mestinya.

Tangerang, 9 Mei 2018



(Christofer Derian Budianto)

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa, karena hanya dengan berkat dan rahmat-Nya lah, skripsi dengan judul **"IMPLEMENTASI KRIPTOGRAFI KURVA ELIPTIK DAN STEGANOGRAFI LEAST SIGNIFICANT BIT UNTUK PENYIMPANAN IDENTITAS"** ini dapat diselesaikan. Penulisan skripsi ini merupakan syarat kelulusan pada Program Studi Informatika Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.

Atas bimbingan, dan saran yang telah diberikan selama proses penulisan skripsi, ucapan terimakasih disampaikan kepada:

1. Dr. Ninok Leksono, selaku Rektor Universitas Multimedia Nusantara,
2. Hira Meidia, Ph.D., selaku Dekan Fakultas Teknik dan Informatika,
3. Seng Hansun, S.Si., M.Cs., selaku Ketua Program Studi dan dosen pembimbing dalam penyusunan skripsi, yang telah membimbing dan membagi ilmunya selama penulisan skripsi,
4. Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, CEH, selaku dosen pembimbing dalam penyusunan skripsi, yang telah membimbing dan membagi ilmunya selama penulisan skripsi,
5. Ayah, ibu, dan seluruh keluarga yang selalu mendoakan dan memberi dukungan moral dari awal hingga akhir penulisan skripsi,
6. Febrian Wilson, Nathania Elvina, Rakadetyo Alif, Kevin Alexander, Willy William, dan Keshia Tiffany yang telah membantu dalam penyelesaian skripsi, baik secara langsung maupun tidak,

7. Ang Rahma, Indah Novia, Enrico Nathaniel, Janssen, Ferdinand, Yudha Teguh Hartanto, Kenny Wantara, Albert Kosasi, Astrid Tamara, Marisa Tri Utami, Tri Nita, Klara Livia, Nesa Alicia, Yosua Winata, Monique Subandi, Viktor, Vicky Reynaldo, Cynthia Sinly dan Gisela Felicia yang telah memberikan bantuan dan dukungan moral selama pengerjaan skripsi,
8. Teman-teman Laboratorium B507 yang telah membantu dalam pengerjaan skripsi,
9. Teman-teman di Program Studi Informatika Universitas Multimedia Nusantara, yang telah menjadi rekan belajar dan berdiskusi selama berkuliah di Universitas Multimedia Nusantara, dan
10. Seluruh pihak lain yang tidak dapat disebutkan satu per satu, yang telah membantu, mendukung, memberi semangat dalam penulisan skripsi.

Semoga skripsi ini dapat memberikan manfaat bagi para pembaca.

Tangerang, 9 Mei 2018

Christofer Derian Budianto

IMPLEMENTASI KRIPTOGRAFI KURVA ELIPTIK DAN STEGANOGRAFI LEAST SIGNIFICANT BIT UNTUK PENYIMPANAN IDENTITAS

ABSTRAK

Pencurian identitas merupakan masalah keamanan yang serius. Kerugian yang ditimbulkan akibat pencurian identitas tidak hanya berupa kerugian materiil namun juga kerugian non materiil seperti kerugian sosial. Di Indonesia, identitas yang resmi diakui di seluruh Negara Kesatuan Republik Indonesia, adalah Kartu Tanda Penduduk (KTP) Indonesia. Untuk mengamankan identitas tersebut dapat digunakan metode kriptografi dan steganografi sehingga identitas terlindungi oleh dua lapisan keamanan. Kriptografi merupakan teknik untuk mengubah suatu informasi menjadi samar agar tidak mudah dipahami oleh orang lain. Kriptografi kurva eliptik merupakan algoritma kriptografi kunci publik yang memanfaatkan kurva elips matematis. Steganografi merupakan teknik untuk menyembunyikan data agar keberadaannya tidak diketahui oleh orang lain. Steganografi *least significant bit* merupakan algoritma untuk menyembunyikan data pada *least significant bit* dari suatu citra digital. Pengujian menunjukkan bahwa *cipher text* yang dihasilkan selalu dua kali lebih panjang dari *plain text*. Hasil rata-rata PSNR yang dihasilkan sebesar 64.97. Nilai tersebut menunjukkan bahwa hasil keluaran aplikasi memiliki tingkat kemiripan yang tinggi.

Kata Kunci: identitas, kriptografi, kriptografi kurva eliptik, *least significant bit*, steganografi

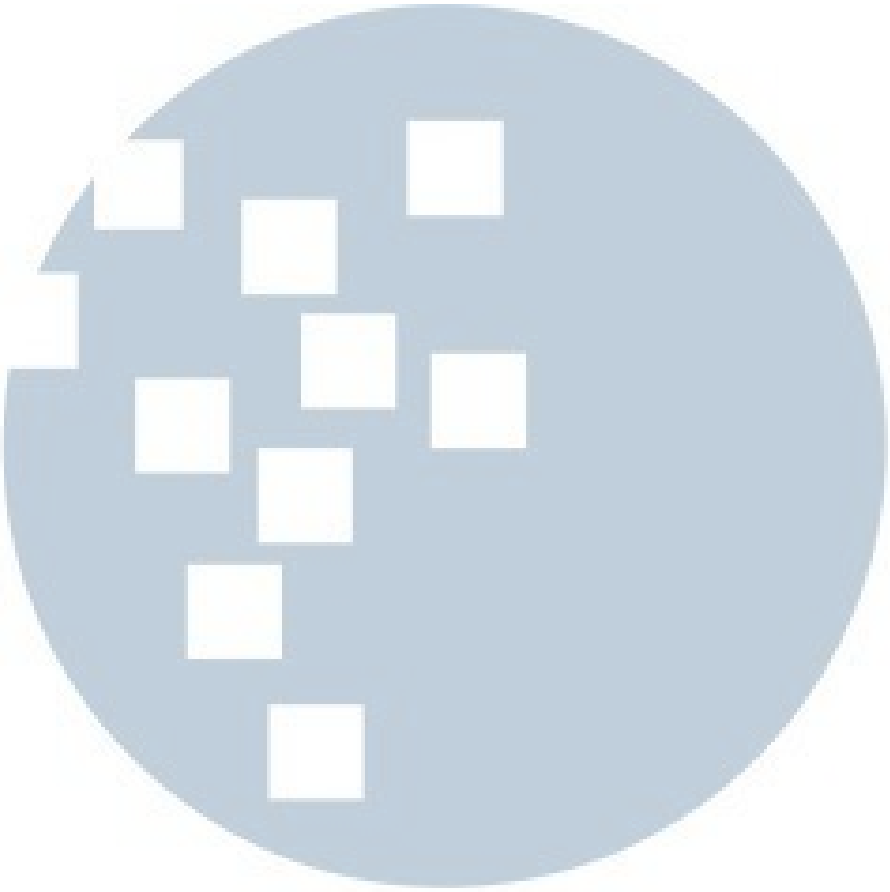
IMPLEMENTATION OF ELLIPTICAL CURVE CRYPTOGRAPHY AND LEAST SIGNIFICANT BIT STEGANOGRAPHY FOR SECURING IDENTITY

ABSTRACT

Identity theft is one of the most serious security threats. Identity theft could cause not only financial loss but also social loss. Indonesia officially recognizes Kartu Tanda Penduduk (KTP) as the legal identity card for its citizens. In order to keep the identity secure, cryptography and steganography used to provide two layers of protection. Cryptography is a technique to change an information into a secret, so as not easily understood by others. Elliptical curve cryptography is a cryptography that uses mathematical elliptic curve. Steganography is a technique to hide data so that its existence is not known by others. Least significant bit steganography is an algorithm that hides data in the least significant bit of a file. The implementation and testing show that the proposed methods are successful for securing identity. The length of cipher text is twice of the plain text. The average PSNR value obtained from the implementation of LSB method is 64.97. The result show that the output is acceptable in terms of security of the ECC and also obscurity of the LSB.

Keywords: cryptography, elliptical curve cryptography, identity, least significant bit, steganography

DAFTAR ISI



DAFTAR RUMUS

DAFTAR GAMBAR

DAFTAR TABEL