KAJIAN PEMBUATAN TANDA-TANGAN DIGITAL DENGAN MENGGUNAKAN *DIGITAL SIGNATURE ALGORITM* (DSA)

SKRIPSI

Sebagai Salah Satu Syarat Memperoleh
Gelar Sarjana Matematika

Oleh :

Lia Andriyani
08011281320010

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS SRIWIJAYA

JANUARI 2018

LEMBAR PENGESAHAN

KAJIAN PEMBUATAN TANDA-TANGAN DIGITAL DENGAN MENGGUNAKAN *DIGITAL SIGNATURE ALGORITM* (DSA)

SKRIPSI

Sebagai Salah Satu Syarat Memperoleh Gelar
Sarjana Matematika Bidang Studi Matematika

Oleh

LIA ANDRIYANI
08011281320010

Indralaya, Desember 2017

Pembimbing Pembantu	Pembimbing Utama
Des Alwine Zayanti, M.Si	**Novi Rustiana Dewi, M.Si**
NIP. 197001113 199603 2 001	**NIP. 19730719 199603 2 002**

Mengetahui
Ketua Jurusan Matematika

Drs. Sugandi Yahdin, M.M
NIP 19580727 198603 1 003

ii

HALAMAN PERSEMBAHAN

Allah akan mengangkat (derajat) orang-orang yang beriman diataramu dan orang-orang yang diberi ilmu beberapa derajat. Dan Allah maha meneliti apa yang kamu kerjakan.

(Q.S. Al-Mujadalah :11)

“Hambatan tidak bisa menghentikan Anda. Masalah tidak bisa menghentikan Anda. Orang lain tidak bisa menghentikan Anda. Hanya Anda yang dapat menghentikan Anda”

(Jeffrey Gitomer)

“Waktu akan selalu tersedia bagi mereka yang memanfaatkannya”

(Leonardo da Vinci)

Skripsi ini kupersembahkan kepada :

- **Allah SWT**
- **Idolaku Nabi Muhammad SAW**
- **Kedua Orang Tuaku tercinta**
- **Kakak-kakaku Tersayang**
- **Para Permberi Ilmu**
- **Sahabat dan Teman-temanku**
- **Almamaterku**

KATA PENGANTAR

Dengan menyebut nama Allah Swt, Tuhan Maha Pengasih dan Maha Penyayang. Puji syukur penulis panjatkan kepada Allah SWT karena atas berkat rahmat, karunia, kasih sayang, dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul **Kajian Pembuatan Tanda-Tangan Digital Menggunakan *Digital Signature Algorithm* (DSA)** sebagai salah satu syarat untuk memperoleh gelar Sarjana Sains Bidang Studi Matematika di Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sriwijaya.

Shalawat serta salam semoga senantiasa tercurah atas Rasul pilihan yang telah bersabda, “Tidak beriman salah seorang kalian sampai dia mencintai saudaranya, seperti dia mencintai dirinya sendiri" (HR. Bukhari dan Muslim).

Selama penyusunan skripsi ini penulis banyak mendapatkan saran, petunjuk dan bantuan dari berbagai pihak mulai dari tahap awal hingga proses penyelesaian. Pada kesempatan ini, dengan segala hormat, cinta dan kerendahan hati penulis mengucapkan terimakasih yang tak terhingga kepada kedua orangtua penulis yakni, **Ibu Yahmi** dan **Alm. Bapak Supriyono**, serta **kakak-kakak**. Terimakasih atas cinta, doa, saran, dan dukungannya yang tak pernah berhenti. Tak lupa penulis mengucapkan terimakasih yang sebesar-besarnya untuk semua pihak yang telah membantu baik secara langsung maupun tidak langsung, kepada yang terhormat :

1. Bapak **Drs.Sugandi Yahdin, M.M,** selaku Ketua Ketua Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sriwijaya yang

telah memberikan arahan,izin, serta kelancaran pelayanan akademik kepada penulis dalam menyusun skripsi.

2. Ibu **Des Alwine Zayanti, M.Si** selaku Sekretaris Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sriwijaya, terimakasih atas bimbingan serta kelancaran pelayanan dalam urusan akademik.
3. Ibu **Novi Rustiana Dewi, M.Si** selaku Pembimbing Utama dan Ibu **Des Alwine Zayanti, M.Si** selaku Pembimbing Pembantu. Terimakasih penulis ucapkan yang sebesar-besarnya karena telah bersedia menyediakan waktu, pikiran, motivasi dan saran serta kesabaran memberikan arahan dan bimbingan terbaik kepada penulis hingga terselesainya skripsi ini.
4. Ibu **Dr. Yulia Resti, M.Si,** Ibu **Indrawati, M.si,** dan Ibu **Ning Eliyati, M.Pd** selaku Penguji utama yang telah bersedia meluangkan waktu dalam memberikan tanggapan, kritik dan saran yang bermanfaat dalam perbaikan dan penyelesaian skripsi ini.
5. Bapak **Drs. Ali Amran, M.T** selaku Dosen Pembimbing Akademik , terimakasih karena telah bersedia memberikan saran, didikan,serta motivasi selama penulis menuntut ilmu di Jurusan Matematika ini.
6. **Seluruh Dosen** Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sriwijaya yang telah memberikan ilmu kepada penulis selama masa perkuliahan.
7. Kak **Irwan,** Ibu **Hamidah,** dan **Semua Pegawai** di Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sriwijaya yang

tidak dapat ditulis satu persatu, terima kasih atas bantuan yang telah diberikan kepada penulis.

8. Kakak-kakakku tercinta yakni **Mas Suryono**, **Mas Sabarudin, Mas Nur Alim, Mbak Muliyanti,** dan **Mbak Lilik puspita Sari**. Terimakasih atas kasih sayang, bimbingan, dan dukungan yang selalu kalian berikan.
9. Sahabatku **Sri Utami**, terimakasih telah menjadi sahabat terbaikku, selalu mendengarkan keluh kesahku, memberikan saran-saran dan dukungan serta motivasi.
10. Sahabat dalam suka dan duka, **Honesty Nabila**. Terimakasih sudah menjadi teman senasib dan seperjuangan selama kuliah. Semoga apa yang menjadi impian dan cita-cita kita dapat terwujud.
11. Sahabatku **Maey Anicha Putri, Yusi Handayani, Rachma Diana, Gita Riski**, Terimakasih atas motivasi, doa, dan dukungannya.
12. Sahabatku **Lita, Delta, Bayu, Ika, Kelly, Ria, Mbak Kia, Mbak Vinda**. Terimakasih atas saran dan dukungannya selama ini.
13. Teman-Teman **Jurusan Matematika Angkatan 2013** serta semua pihak yang tidak dapat disebutkan satu persatu. Terimakasih atas kebersamaannya selama ini, semoga kita semua menjadi orang yang sukses. Aamiin

Semoga Allah SWT melimpahkan rahmat-Nya kepada semua pihak yang telah membantu, memberi nasehat, serta membimbing saya. Semoga skripsi ini bermanfaat dan dapat menambah pengetahuan bagi kita semua. Aamiin.

Indralaya, Januari 2018

Penulis

STUDY DIGITAL SIGNATURE MANAGEMENT USING *DIGITAL SIGNATURE ALGORITHM* (DSA)

By :

LIA ANDRIYANI
08011281320010

ABSTRACT

Digital signatures are a cryptography value that depends on message and message sender. One method of making digital signatures is to use DSA. DSA is an asymmetric key cryptography because it uses two keys namely a private key and a public key. The digital signature is used to reassure the recipient that the received message is still original or unmodified. There are three main steps in making digital signatures using DSA: key generation, signature handling, and verification of signature validity. In this research obtained public key pair $(p, q, g, y) = (59419,3301,36378,38288)$. With the same key obtained different signature for every different secret message and when verifying with the same public key obtained $v = r$ but for messages that have been changed at the time of veificafion $v \neq r$.

Keywords : Cryptography, Digital Signature, DSA, Hash Value, Public key, Private key.

KAJIAN PEMBUATAN TANDA-TANGAN DIGITAL MENGGUNAKAN *DIGITAL SIGNATURE ALGORITHM* (DSA)

Oleh :
LIA ANDRIYANI
08011281320010

ABSTRAK

Tanda-tangan digital merupakan sebuah nilai kritptografis yang bergantung pada pesan dan pengirim pesan. Salah satu metode dalam pembuatan tanda-tangan digital yaitu dengan menggunakan DSA. DSA merupakan kriptografi kunci asimetris karena menggunakan dua buah kunci yaitu kunci rahasia dan kunci publik. Tanda-tangan digital digunakan untuk meyakinkan penerima pesan bahwa pesan yang diterima masih asli atau belum dimodifikasi. Terdapat tiga langkah utama dalam pembuatan tanda-tangan digital menggunakan DSA yaitu pembangkitan kunci, pembuatan tanda-tangan, dan verifikasi keabsahan tanda-tangan. Pada penelitian ini diperoleh pasangan kunci publik $(p, q, g, y) = (59419,3301,36378,38288)$ dengan kunci rahasia $x = 2759$. Dengan kunci yang sama dapat menghasilkan tanda-tangan yang berbeda untuk setiap pesan rahasia yang berbeda dan saat diverifikasi dengan kunci publik yang sama dapat menghasilkan $v = r$ tetapi untuk pesan yang telah diubah pada saat verifikasi menghasilkan $v \neq r$.

Kata kunci : Kriptografi, Tanda-tangan digital, DSA, Nilai Hash, Kunci publik, Kunci Rahasia.

DAFTAR ISI

Halaman

BAB I

PENDAHULUAN

I.I Latar Belakang

Perkembangan teknologi informasi dan komunikasi berkembang sangat pesat seiring dengan perkembangan zaman yang semakin modern. Tidak dapat dihindari bahwa setiap hari dibutuhkan pertukaran informasi dengan orang lain baik itu informasi umum maupun rahasia. Tingkat kebutuhan akan pertukaran informasi dan pesan yang sangan tinggi ini mendorong peneliti untuk menciptakan suatu media yang dapat digunakan untuk bertukar informasi dan pesan secara mudah dan cepat. Seperti yang diketahui saat ini pertukaran informasi dan pesan menggunakan jaringan selular dan internet. Namun seiring perkembangan internet yang semakin canggih dan ekonomis maka jaringan selular semakin banyak ditinggalkan dan beralih ke jaringan internet.

Dengan internet maka pertukaran pesan akan semakin mudah dan murah. Namun, semakin banyaknya pengguna internet mengakibatkan internet menjadi tidak terlalu aman untuk bertukar pesan yang bersifat rahasia karena internet dapat diakses oleh siapapun sehingga memungkinkan ada pihak yang tidak bertanggung jawab dapat mencuri dan meubah pesan rahasia yang dikirim. Berbagai cara dilakukan untuk menjamin kerahasiaan dan keaslian pesan. Untuk menjaga kerahasiaan pesan biasanya dengan cara meubah pesan menjadi kode-kode yang sulit dimengerti, apabila ada pihak yang mencuri informasi rahasia yang dikirim akan kesulitan dalam memahami isi pesan rahasia tersebut.

Namun,dengan hanya menyandikan pesan saja tidak akan cukup untuk menjaga keaslian pesan rahasia yang dikirim. Untuk menjaga keaslian pesan diperlukan sebuah tanda-tangan digital yang dapat meyakinkan penerima pesan bahwa pesan yang diterima masih asli. Untuk mengatasi masalah diatas diperlukan kriptografi yang dapat digunakan untuk menyandikan pesan rahasia dan membuat tanda tangan digital.

Ada beberapa algoritma yang dapat digunakan dalam pembuatan tanda-tangan digital, diantaranya RSA *signature,* ElGamal *Signature,* dan DSA (*Digital signature Algoritm*). Pada penelitian ini akan diteliti tentang DSA. DSA adalah algoritma yang digunakan dalam DSS (*Digital Signature Standard*). DSS adalah bakuan untuk tanda-tangan digital yang diresmikan pada bulaan agustus 1991 oleh NITS (*National Institute of Standard and Tecnology*). DSA tidak dapat digunakan dalam proses enskripsi pesan, DSA dispesifikasikan khusus untuk penbuatan tanda-tangan digital.

Ada beberapa penelitian yang telah membahas tentang pembuatan tanda-tangan digital seperti, Rinaldi Ulfa Ariska (2011) dalam skripsinya yang membahas tentang penerapan sistem kriptografi ElGamal atas Z_p^* dalam pembuatan tanda-tangan digital. Pada penelitian ini terdapat kelemahan pada perhitungan *hash* terdapa *collision. Hash* adalah pengubahan suatu string yang panjangnya sembarang menjadi ukurannya tetap yang merepresentasikan string aslinya. Apabila dari dua pesan yang berbeda tetapi menghasilkan *hash* yang sama, hal ini disebut dengan *collision*. Selain itu, Nora Hendrawati dkk. (2008) menuliskan perancangan dan implementasi DSA menggunakan bahasa pemrograman java. Dalam penelitian ini diperoleh hasil sebuah

program yang diberi nama SimDSA dengan kemampuan untuk membangkitkan pasangan kunci, membangkitakan tanda-tangan digital, dan memverifikasi tanda-tangan digital.

Dari penelitian di atas, dalam penelitian ini dibahas pembuatan tanda-tangan digital menggunakan DSA serta perhitungan matematis berdasarkan pada kajian teori bilangan. Selain itu akan dibahas juga mengenai perhitungan nilai *hash* pada pesan rahasia agar tidak terjadi *collision.*

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, dapat dirumuskan permasalahan sebagai berikut :

1. Bagaimana proses pembangkitan kunci publik (*public key*) dan kunci rahasian (*privat key*) pada DSA ?
2. Bagaimana proses penandatanganan pesan mengguanakan DSA ?
3. Bagaimana memverifikasi keaslian pesan dengan mennggunakan DSA ?
4. Bagaimana hasil dari verifikasi pesan rahasia yang telah terkena serangan *cryptanalish* ?

1.3 Pembatasan Masalah

Dalam penelitian ini dibahas mengenai perhitungan matematis berdasarkan pada kajian ilmu teori bilangan dalam pembuatan tanda-tangan digital dan memverifikasi pesan yang diterima menggunakan DSA serta perhitungan nilai *hash*

menggunakan program MD5 online. Materi yang dibahas dalam penelitian ini tidak berlaku umum, hanya berdasarkan kasus yang diambil.

1.4 Tujuan

Tujuan dari penelitian ini adalah :

1. Untuk memperoleh pasangan kunci pubik (*public key*) dan kunci rahasian (*privat key*).
2. Untuk memperoleh tanda-tangan digital dari pesan yang akan dikirimkan.
3. Untuk meyakinkan penerima pesan bahwa pesan yang diterima masih asli atau sudah diubah.
4. Untuk mengetahui hasil verifikasi dari pesan yang terkena serangan *cryptanalish.*

1.5 Manfaat

penelitian ini diharapkan dapat membantu pembaca memahami tentang pembuatan tanda-tangan digital menggunakan DSA serta kajian ilmu teori bilangan yang melandasinya.

DAFTAR PUSTAKA

Ariska, Rinaldi Ulfa. 2011. *Penerapan Sistem Kriptografi ElGamal atas Z_p^* dalam Pembuatan Tanda-Tangan Digital*. Yogyakarta: UNY.

Buchmann, Johannes A. 2000. *Introduction to Cryptography*. New York : Springer-Verlag.

Hendrawati Nora, dkk. 2008. *Perancangan dan Implementasi DSA Menggunakan Bahasa Pemrograman Java*. Semarang: Universitas Diponegoro.

Maryanto Budi. 2008. *Penggunaan Fungsi Hash Satu-Arah Untuk Enkripsi Data*. Bandung: Media Informatika.

Menezes, Oorcshot, and Vanstone. 1996. *Handbook of Applied Cryptography*. Florida : CRC Press.

Munir, Rinaldi. 2005. *Penggunaan Tanda-Tangan Digital Untuk Menjaga Integritas Berkas Perangkat Lunak*. Yogyakarta: SNATI.

Mujaddid, Sibghatullah. 2009. *Kriptoanalisis Pada Fungsi Hash Kriptografi MD5*. Bandung: Teknik Informatika ITB

Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Informatika Bandung.

Munir, Rinaldi. 2014. *Matematika Diskrit*. Bandung : Informatika Bandung.

Niven Ivan,dkk. 1991. *An Introduction to The Theory Of Numbers*. United States: Courier Companies.

Stinson, Douglas R.1995. *Cryptography Theory and Practice*.United States: CRC press.

Sukirman. 2006. *Pengantar Teori Bilangan.* Yogyakarta : Hanggar Kreator.

Thakkar, J. 2015. An Encryption and Decryption More Secure Elgamal Cryptosystem. *International Journal of Science Technology & Engineering* , 119.