AUTENTIKASI DOKUMEN DIGITAL DENGAN MENGGUNAKAN *SECURE HASH ALGORITHM-256* DAN *ELGAMAL SIGNATURE SCHEME*

Skripsi

Diajukan untuk memenuhi sebagian syarat untuk memperoleh

Gelar Sarjana Matematika

Oleh:

Yopi Robi Milenium

1600697

PROGRAM STUDI MATEMATIKA

DEPARTEMEN PENDIDIKAN MATEMATIKA

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2020

LEMBAR HAK CIPTA

AUTENTIKASI DOKUMEN DIGITAL DENGAN MENGGUNAKAN *SECURE HASH ALGORITHM*-256 DAN *ELGAMAL SIGNATURE SCHEME*

Oleh:

Yopi Robi Milenium

NIM 1600697

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

LEMBAR PENGESAHAN

YOPI ROBI MILENIUM

AUTENTIKASI DOKUMENTASI DIGITAL DENGAN MENGGUNAKAN *SECURE HASH ALGORITHM*-256 DAN ELGAMAL *SIGNATURE SCHEME*

Disetujui dan disahkan oleh pembimbing:

Pembimbing I

acc sidang

Dra. Hj. Rini Marwati, M.S.

NIP. 196606251990012001

Pembimbing II

Hj. Dewi Rachmatin, S.Si., M.Si.

NIP. 196909291994122001

Mengetahui,

Ketua Departemen Pendidikan Matematika

Dr. H. Dadang Juandi, M.Si.

NIP. 196401171992021001

ABSTRAK

"Autentikasi Dokumen Digital dengan Menggunakan *Secure Hash Algorithm*-256 dan *ElGamal Signature Scheme*".

Sekarang ini, membuat dokumen tidak diproduksi hanya berupa cetakan melainkan dapat disajikan juga dalam bentuk digital. Keamanan suatu dokumen digital sangat perlu diperhatikan, karena tidak menutup kemungkinan pada saat proses pengiriman dokumen tersebut telah terjadi campur tangan pihak ketiga yang tidak bertanggung jawab yang mengubah atau memalsukan dokumen tersebut. Penelitian ini bertujuan untuk menjelaskan bagaimana prosedur autentikasi dokumen digital menggunakan kombinasi dua algoritma, yaitu *Secure Hash Algorithm-256* dan *ElGamal Signature Scheme* serta merancang program aplikasinya dengan bahasa pemrograman Python. Hasil dari penelitian menunjukkan bahwa kombinasi algoritma *Secure Hash Algorithm*-256 dan *ElGamal Signature Scheme* dapat dirancang menjadi sebuah program aplikasi untuk autentikasi dokumen digital. Program aplikasi ini dapat mempermudah pengguna untuk membuat tanda tangan digital, serta melakukan autentikasi dokumen digital.

Kata Kunci: Dokumen digital, kriptografi, tanda tangan digital, autentikasi, *Secure Hash Algorithm*-256, *ElGamal Signature Scheme*

ABSTRACT

"Digital Document Authentication with Secure Hash Algorithm-256 and ElGamal Signature Scheme"

Nowadays, document is not only produced in printed form, but also can be presented in digital form. The security of digital document really needs to be considered, because it does not rule out the possibility that during the process of sending document there has been interference by a third party who is not responsible for changing or falsifying the document. This research aims to explain how procedure uses two algorithms, namely Secure Hash Algorithm-256 and the ElGamal Signature Scheme and designing the application program with the Python programming language.

The result of this research indicated that the combination of Secure Hash Algorithm-256 and the ElGamal Signature Scheme can be designed to be an application program for digital document authentication. This application program can make it easier for users to create digital Signatures, as well as perform digital document authentication.

Keywords: *Digital Document, cryptography, digital signature, authentication, Secure Hash Algorithm-256, ElGamal Signature Scheme*

DAFTAR ISI

DAFTAR PUSTAKA

Ariyus, Dony. (2008). *Pengantar Kriptografi*. Yogyakarta: Andi.

Burton, M. David. (2007). *Elementary Number Theory, Sixth Edition.* New York: The McGraw-Hill Companies, Inc.

Dafi. (2018). *Apa itu File PDF dan Bagaimana Cara Membuat File PDF*. (Diakses pada 2020 November 11). Tersedia pada: https://www.dafideff.com/2018/09/apa-itu-file-pdf-dan-bagaimana-cara-membuat-file-pdf.html

Alfin, F. (2019). *Dasar Pemrograman Python Untuk Pemula.* (Diakses pada 2020 November 11). Tersedia pada: https://halovina.com/dasar-pemrograman-python-untuk-pemula/

Kendal. (2003). *Software Engineering: a Practicioner Approach.* Penerbit : The McGraw-Hill Companies, Inc.

Mollin, R. A. (2007). *An Introduction to Crypthography Second Edition.* New York: CRC Press.

Munir, R. (2005). *Teori Bilangan Bahan Kuliah IF2151.*

Munir, R. (2006). *Kriptografi*. Bandung: Informatika Bandung.

Munir, R. (2017). *Tandatangan Digital Bahan Kuliah IF4020 Kriptografi.*

Niven, I., et. al. (1991). *An Introduction to The Theory of Number Fifth Edition.* Canada: Courier Companies, Inc.

Pungky dan Ahmad. (2015). *Aplikasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma Message Digest 5 (MD5)*. Vol. 5 No. 1 Edisi Mei 2015.

Rahmawati dan Agus. (2009). *Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi pada e-Voting Indonesia*. Seminar Nasional Informatika UPN "Veteran" Yogyakarta.

Rosen, K.H. (2011). *Elementary Number Theory and its applications 6th Edition.* Boston: Pearson Education, Inc.

Sandeep, Shikhar et. al. (2020). *Python Bitwise Operators.* (Diakses pada 2020 November 12). Tersedia pada: https://www.geeksforgeeks.org/python-bitwise-operators/

Stalling, W. (2005). *Crypthography and Network Security Principles.*

Stinson, D. R. (2006). *Cryptography*: *Theory and Practice Third Edition*. Florida: CRC Press.

Sukarman, H. (2001). *Teori Bilangan*, Penerbit: Universitas Terbuka.

Sutopo, Sahl Fawzy. (2020). Implementasi *Digital Signature Algorithm* (DSA) menggunakan *Secure Hash Algorithm*-256 pada Media Gambar. Skripsi. FPMIPA, Universitas Pendidikan Indonesia, Bandung.

Yahdiani, E. dan Rizky. 2018. *Implementasi Algoritma AES 128 dan SHA-256 dalam Pengkodean pada Sebagian Frame Video CCTV MPEG-2*. JATIKOM Vol. 1 No. 1 hal. 33-39.

Yauris K. (2015). *Penggunaan Fungsi Hash dan Tanda Tangan Digital Digital dalam Transmisi Data*, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Bandung.