DIGITAL SIGNATURE MENGGUNAKAN SHA-256 DENGAN SKEMA PENANDATANGANAN DIFFIE-HELLMAN-RSA

Skripsi

Diajukan untuk memenuhi sebagian syarat untuk memperoleh

Gelar Sarjana Matematika

oleh:

Muhammad Agus Hermawan

NIM 1702229

PROGRAM STUDI MATEMATIKA

DEPARTEMEN PENDIDIKAN MATEMATIKA

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2021

LEMBAR HAK CIPTA

DIGITAL SIGNATURE MENGGUNAKAN SHA-256 DENGAN SKEMA PENANDATANGANAN DIFFIE-HELLMAN-RSA

Oleh
Muhammad Agus Hermawan

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

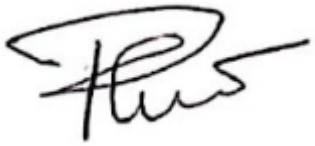
LEMBAR PENGESAHAN

MUHAMMAD AGUS HERMAWAN

DIGITAL *SIGNATURE* MENGGUNAKAN SHA-256 DENGAN SKEMA PENANDATANGANAN DIFFIE HELLMAN-RSA

disetujui dan disahkan oleh pembimbing:

Pembimbing I,

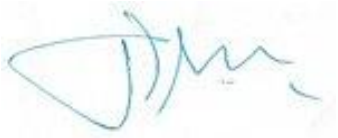


Dra. Hj. Rini Marwati M.S.
NIP. 196606251990012001

Pembimbing II,

Ririn Sispiyati, S.Si., M.Si.
NIP. 198106282005012001

Mengetahui,
Ketua Departemen Pendidikan Matematika



Dr. H. Dadang Juandi, M.Si.
NIP. 196401171992021001

Digital Signature Menggunakan SHA-256 dengan Skema Penandatanganan Diffie-Hellman-RSA

ABSTRAK

Keaslian suatu dokumen adalah suatu hal yang sangat penting, terlebih lagi jika dokumen tersebut berbentuk sertifikat. Pada era yang serba digital, sertifikat juga dapat diubah ke dalam bentuk digital, namun pada kenyataannya sertifikat digital ini mudah sekali dipalsukan. Sertifikat digital dapat diperiksa keasliannya dengan banyak metode, salah satunya adalah *digital signature*. Dalam pengimplementasiannya, metode *digital signature* ini dapat menggunakan berbagai algoritma begitupun skema penandatanganannya dapat menggunakan berbagai algoritma kriptografi. Dalam penelitian ini diimplementasikan metode *digital signature* dengan menggunakan algoritma SHA-256 dan skema penandatanganan Diffie-Hellman-RSA. Algoritma SHA-256 dipilih karena cukup aman dan merupakan pengembangan dari SHA sebelumnya, sementara skema penandatanganan Diffie-Hellman-RSA dipilih karena merupakan pengembangan dari RSA, sehingga lebih sulit dilakukan kriptanalisis. Dalam melakukan kriptanalisis pada algoritma Diffie-Hellman-RSA diharuskan untuk memfaktorkan kunci publik menjadi 3 buah bilangan prima sementara pada RSA hanya memfaktorkan kunci publik menjadi 2 buah bilangan prima. Untuk mempermudah melakukan pengecekan keaslian sertifikat digital dibuatlah suatu program aplikasi yang dapat membedakan sertifikat yang asli dan yang palsu, program ini memberikan *digital signature* berupa *string* angka pada sertifikat digital, dan memberikan *output* akhir berupa keaslian suatu sertifikat digital.

Kata Kunci: Sertifikat Digital, *Digital Signature*, *SHA*, *Diffie-Hellman*, *RSA*.

Digital Signature Using SHA-256 with the Diffie-Hellman-RSA Signing Scheme

ABSTRACT

The authenticity of a document is very important, especially if the document is in the form of a certificate. In this digital era, certificates can also be converted into digital form, but in reality these digital certificates are very easy to fake. Digital certificates can be authenticated by many methods, one of which is a digital signature. In its implementation, this digital signature method can use various algorithms as well as the signing scheme can use various cryptographic algorithms. In this research, a digital signature method is implemented using the SHA-256 algorithm and the Diffie-Hellman-RSA signing scheme. The SHA-256 algorithm was chosen because it is quite secure and is a development of the previous SHA, while the Diffie-Hellman-RSA signing scheme was chosen because it is development of RSA, so it is more difficult to cryptanalyze. In doing cryptanalysis on Diffie-Hellman-RSA algorithm is required to factorizes the public key into 3 prime numbers while RSA only factorizes the public key into 2 prime numbers. To make it easier to check the authenticity of digital certificates, an application program is made that can distinguish genuine and fake certificates, this program provides a digital signature in the form of a string of numbers on a digital certificate, and provides the final output in the form of the authenticity of a digital certificate.

Kata Kunci: *Digital Certificate , Digital Signature, SHA, Diffie-Hellman, RSA*

DAFTAR ISI

DAFTAR PUSTAKA

Adleman, L., Rivest, R. L., & Shamir, A. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystem .

Alajbegović, H., Jamak, H., & Zečić, D. (2006). Digital Signature Algorithm (DSA). *10th International Research/Expert Conference*, 665-668.

Burton, D. M. (2011). *Elementary Number Theory Seventh Edition.* New York: McGraw-Hill.

Cameron, P. J. (2003). *Notes on cryptography.* London: Queen Mary, University of London.

Gupta, P., & Kumar, S. (2014). A Comparative Analysis of SHA and MD5. *International Journal of Computer Science and Information Technologies*, 4492 - 4495.

Merkle, R. C. (1978). Secure Communications Over Insecure Channels. *Communications of the ACM*, 294-299.

Millenium, Y. R. (2020). Autentikasi Dokumen Digital Dengan Menggunakan Secure Hash Algorithm-256 dan Elgamal Signature Scheme.

Munir, R. (2004). Teori Bilangan (Number Theory) Bahan Kuliah IF5054.

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

Munir, R. (2018). Fungsi Hash Bahan Kuliah IF4020 Kriptografi.

Munir, R. (2018). Tanda tangan Digital Bahan Kuliah IF4020 Kriptografi.

National Institute of Standards and Technology (NIST). (1994). Digital Signature Standard (DSS).

National Institute of Standards and Technology (NIST). (2015). *Secure Hash Standard (SHS).* Gaithersburg: Federal Information Processing Standards.

Nisha, S., & Farik, M. (2017). RSA Public Key Cryptography Algorithm - A Review. *International Journal of Scientific & Technology Research Volume 6, Issue 07*, 187-191.

Niven, I., Zuckerman, H. S., & Montgomery, H. L. (1991). *An Introduction to the Theory of Numbers.* Michigan: University of Michigan.

Rijmen, V., & Oswald, E. (2005). Update on SHA-1.

Sobti, R., & Geetha, G. (2012). Cryptographic Hash Functions: A Review. *International Journal of Computer Science Issues* , 461- 479.

Srinath, K. (2017). Python – The Fastest Growing Programming Language. *International Research Journal of Engineering and Technology*, 354-357.

Stinson, D. R., & Paterson, M. B. (2018). *Cryptography Theory and Practice Fourth Edition.* London: CRC Press.

Susanto, H., Setiawan, C., & Wardhani, W. B. (2013). Digital Signature Algorithm (DSA). 1-13.

Sutopo, S. F. (2020). Implementasi Digital Signature Algorithm (DSA) Menggunakan Secure Hash Algorithm-256 (SHA-256) Pada Media Gambar.

Vincent, P. M. (2016). Hybrid Security Approach by Combining Diffie-Hellman and RSA algorithms. *International Journal of Pharmacy & Technology*, 26560-26567.