

***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

©Muhammad Agus Hermawan 2021  
Universitas Pendidikan Indonesia  
2021

Hak Cipta dilindungi undang-undang

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,  
dengan dicetak ulang, difotokopi atau cara lainnya tanpa izin dari penulis

**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

LEMBAR PENGESAHAN .....	
LEMBAR PERNYATAAN .....	
KATA PENGANTAR.....	<b>Error! Bookmark not defined.</b>
ABSTRAK .....	4
ABSTRACT .....	5
DAFTAR ISI .....	6
DAFTAR GAMBAR .....	<b>Error! Bookmark not defined.</b>
DAFTAR TABEL.....	<b>Error! Bookmark not defined.</b>
BAB I PENDAHULUAN .....	<b>Error! Bookmark not defined.</b>
1.1 Latar Belakang Masalah.....	<b>Error! Bookmark not defined.</b>
1.2 Rumusan Masalah.....	<b>Error! Bookmark not defined.</b>
1.3 Batasan Masalah.....	<b>Error! Bookmark not defined.</b>
1.4 Tujuan Penelitian.....	<b>Error! Bookmark not defined.</b>
1.5 Manfaat Penelitian .....	<b>Error! Bookmark not defined.</b>
1.6 Sistematika Penulisan .....	<b>Error! Bookmark not defined.</b>
BAB II LANDASAN TEORI.....	<b>Error! Bookmark not defined.</b>
2.1 Kekongruenan .....	<b>Error! Bookmark not defined.</b>
2.1.1 Kekongruenan (Burton, 2011) .....	<b>Error! Bookmark not defined.</b>
2.1.2 FPB (Burton, 2011).....	<b>Error! Bookmark not defined.</b>
2.1.3 Relatif Prima.....	<b>Error! Bookmark not defined.</b>
2.2 Aritmetika Modulo (Munir, 2004).....	<b>Error! Bookmark not defined.</b>
2.3 Kriptografi.....	<b>Error! Bookmark not defined.</b>
2.4 Kriptografi Kunci Publik.....	<b>Error! Bookmark not defined.</b>
2.5 <i>Digital Signature</i> .....	<b>Error! Bookmark not defined.</b>
2.6 Fungsi Hash.....	<b>Error! Bookmark not defined.</b>
2.7 SHA .....	<b>Error! Bookmark not defined.</b>
2.8 Diffie-Hellman <i>Key Exchange</i> .....	<b>Error! Bookmark not defined.</b>
2.9 ASCII .....	<b>Error! Bookmark not defined.</b>
2.10 RSA.....	<b>Error! Bookmark not defined.</b>
2.10.1 Contoh Pembangkitan Kunci RSA.....	<b>Error! Bookmark not defined.</b>
2.10.2 Contoh Enkripsi RSA.....	<b>Error! Bookmark not defined.</b>
2.10.3 Contoh Dekripsi RSA.....	<b>Error! Bookmark not defined.</b>

2.10.4	Kelebihan dan Kekurangan RSA .....	<b>Error! Bookmark not defined.</b>
2.11	Bahasa Pemrograman Python .....	<b>Error! Bookmark not defined.</b>
BAB III METODE PENELITIAN .....		<b>Error! Bookmark not defined.</b>
3.1	Identifikasi Masalah.....	<b>Error! Bookmark not defined.</b>
3.2	Model Dasar .....	<b>Error! Bookmark not defined.</b>
3.3	Pengembangan Model.....	<b>Error! Bookmark not defined.</b>
3.4	Konstruksi Program Aplikasi .....	<b>Error! Bookmark not defined.</b>
3.4.1	Input dan Output .....	<b>Error! Bookmark not defined.</b>
3.4.2	Rancangan Tampilan.....	<b>Error! Bookmark not defined.</b>
3.4.3	Algoritma <i>Digital signature</i> .....	<b>Error! Bookmark not defined.</b>
3.5	Keamanan <i>Digital Signature</i> dengan Algoritma SHA-256 dan Skema Penandatanganan Diffie-Hellman-RSA .....	<b>Error! Bookmark not defined.</b>
3.6	Validasi .....	<b>Error! Bookmark not defined.</b>
BAB IV HASIL DAN PEMBAHASAN .....		<b>Error! Bookmark not defined.</b>
4.1	Hasil Program.....	<b>Error! Bookmark not defined.</b>
4.1.1	<i>Interface</i> Program .....	<b>Error! Bookmark not defined.</b>
4.1.2	Petunjuk Penggunaan .....	<b>Error! Bookmark not defined.</b>
4.2	Validasi .....	<b>Error! Bookmark not defined.</b>
BAB V KESIMPULAN DAN SARAN .....		<b>Error! Bookmark not defined.</b>
5.1	Kesimpulan.....	<b>Error! Bookmark not defined.</b>
5.2	Saran .....	<b>Error! Bookmark not defined.</b>
DAFTAR PUSTAKA .....		8
LAMPIRAN .....		<b>Error! Bookmark not defined.</b>
Lampiran 1: <i>Coding</i> Program <i>Digital Signature</i> .....		<b>Error! Bookmark not defined.</b>
Lampiran 2: Tabel ASCII <i>Printable Characters</i> .....		<b>Error! Bookmark not defined.</b>

## 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.