

**Implementasi Algoritma Rivest Shamir Adleman dan Algoritma  
Secure Hash Algorithm-256 pada Aplikasi *E-Voting* Berbasis WEB**

**SKRIPSI**

Diajukan untuk memenuhi Sebagian syarat untuk memperoleh gelar Sarjana  
Matematika



Oleh:

Denata Arif Nur Muhamad

1903025

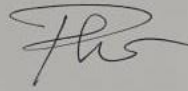
**PROGRAM STUDI MATEMATIKA  
FALKUTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM  
UNIVERSITAS PENDIDIKAN INDONESIA  
2024**

## LEMBAR PENGESAHAN

Denata Arif Nur Muhamad (1903025)

Implementasi Algoritma Rivest Shamir Adleman dan Algoritma Secure Hash  
Algoritma-256 pada Aplikasi *E-voting* Berbasis WEB

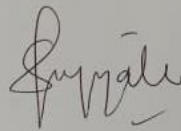
Disetujui dan disahkan,  
Pembimbing I



**Dra. Hj. Rini Marwati, M.S.**

**NIP. 196606251990012001**

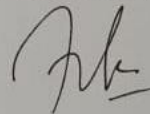
Pembimbing II



**Ririn Sispiyati, S.Si., M.Si.**

**NIP. 198106282005012001**

Mengetahui,  
Ketua Program Studi Matematika



**Dr. Kartika Yulianti, S.Pd., M.Si.**

**NIP. 198207282005012001**

## LEMBAR HAK CIPTA

Implementasi Algoritma Rivest Shamir Adleman dan Algoritma Secure Hash  
Algoritma-256 pada Aplikasi *E-voting* Berbasis WEB

Oleh  
Denata Arif Nur Muhamad

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

© Denata Arif Nur Muhamad 2024  
Universitas Pendidikan Indonesia  
Agustus 2004

Hak Cipta dilindungi undang-undang.  
Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,  
dengan dicetak ulang, difoto kopi, atau cara lainnya tanpa ijin dari penulis.

## ABSTRAK

Pemungutan suara di Indonesia masih menggunakan cara konvensional yang memiliki beberapa kekurangan. Oleh sebab itu, diperlukan cara baru yang lebih efektif dan aman menggunakan *electronic voting* atau biasa disebut dengan *e-voting* yang lebih efektif dan aman. Tujuan penelitian ini merancang dan mengkontruksi aplikasi *e-voting* berbasis web dengan menggunakan kriptografi RSA dan SHA-256. Penggunaan SHA-256 dan RSA pada aplikasi *e-voting* ini untuk membuat tanda tangan digital yang digunakan untuk keabsahan suara pada aplikasi *e-voting*. Pembuatan aplikasi *e-voting* ini dikonstruksi menggunakan bahasa pemrograman *javascript* yang membuat web menjadi *userfriendly* dan menggunakan dua *framework*, yaitu *React.js* dan *Next.js*. Hasil penelitian ini berupa prototipe aplikasi *e-voting* berbasis web yang mengimplementasikan kriptografi RSA dan SHA-256 untuk meningkatkan keamanan pada aplikasi.

**Kata Kunci:** *e-voting*, kriptografi, RSA, SHA-256, *javascript*

## **ABSTRACT**

*Voting in Indonesia still uses conventional methods that have several disadvantages. Therefore, a new way that is more effective and secure is needed using electronic voting or commonly referred to as e-voting which is more effective and secure. This research aims to design and construct a web-based e-voting application using RSA and SHA-256 cryptography. The use of SHA-256 and RSA in this e-voting application is to create a digital signature that is used to validate the vote in the e-voting application. The e-voting application is constructed using javascript programming language that makes the web userfriendly and uses two frameworks, namely React.js and Next.js. The result of this research is a web-based e-voting application prototype that implements RSA and SHA-256 cryptography to increase the security of the application.*

**Keyword:** *e-voting, cryptography, RSA, SHA-256, javascript*

## DAFTAR ISI

<b>LEMBAR PENGESAHAN</b> .....	<b>i</b>
<b>LEMBAR HAK CIPTA</b> .....	<b>ii</b>
<b>LEMBAR PERNYATAAN</b> .....	<b>iii</b>
<b>KATA PENGANTAR</b> .....	<b>iv</b>
<b>UCAPAN TERIMA KASIH</b> .....	<b>v</b>
<b>ABSTRAK</b> .....	<b>vi</b>
<b>ABSTRACT</b> .....	<b>vii</b>
<b>DAFTAR ISI</b> .....	<b>viii</b>
<b>DAFTAR GAMBAR</b> .....	<b>xi</b>
<b>DAFTAR TABEL</b> .....	<b>xii</b>
<b>BAB I PENDAHULUAN</b> .....	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Tujuan Penelitian .....	3
1.4 Manfaat Penelitian .....	4
<b>BAB II KAJIAN PUSTAKA</b> .....	<b>5</b>
2.1 Teori Dasar Matematika .....	5
2.1.1 Pembagi .....	5
2.1.2 Bilangan Prima .....	5
2.1.3 FPB (Faktor Persekutuan Terbesar) .....	5
2.1.4 Relatif Prima .....	5
2.1.5 Teorema <i>Euclidean</i> .....	5
2.1.6 Modulo .....	6
2.1.7 Invers Modulo .....	6
2.1.8 Teorema Euler .....	6
2.2 Kriptografi .....	6
2.2.1 Terminologi Istilah .....	6
2.2.2 Kriptosistem .....	7
2.2.3 Sistem ASCII .....	7
2.2.4 Kriptografi Simetris .....	8
2.2.5 Kriptografi Asimetris .....	8

2.2.6 Protokol Kriptografi.....	9
2.3 Fungsi <i>Hash</i> .....	9
2.5 RSA .....	13
2.6 Digital Signature/Tanda tangan digital .....	15
2.8 E-voting .....	16
2.9 Javascript .....	17
<b>BAB III METODE PENELITIAN .....</b>	<b>18</b>
3.1 Identifikasi Masalah .....	18
3.2 Model Dasar .....	18
3.2.1 SHA-256 .....	18
3.2.2 Kriptografi RSA.....	19
3.2.3 Tanda Tangan Digital .....	19
3.3 Pengembangan Model .....	20
3.4 Perancangan Program Aplikasi .....	21
3.4.1 Input dan Output .....	21
3.4.2 Protokol.....	22
3.4.3 Algoritma Deskriptif.....	22
3.4.4 Rancangan Tampilan Aplikasi Web .....	24
3.4.5 <i>Library</i> Program .....	28
3.5 Proses Validasi.....	28
3.6 Pengambilan Kesimpulan.....	28
<b>BAB IV HASIL DAN PEMBAHASAN.....</b>	<b>29</b>
4.1 Skema Aplikasi <i>E-Voting</i> Menggunakan Algoritma RSA dan SHA-256....	29
4.2 Konstruksi Program Aplikasi <i>E-Voting</i> menggunakan Algoritma RSA dan SHA-256.....	31
4.2.1 <i>Pseudocode</i> Program Aplikasi <i>E-Voting</i> menggunakan Algoritma RSA dan SHA-256 .....	31
4.2.2 Tampilan Program Aplikasi <i>E-Voting</i> menggunakan Algoritma RSA dan SHA-256 .....	34
4.3 Validasi Program Aplikasi <i>E-Voting</i> menggunakan Algoritma RSA dan SHA- 256.....	39
4.3.1 Validasi Proses Registrasi .....	39

4.3.2 Validasi Autentikasi Suara pada Aplikasi E-Voting .....	42
<b>BAB V KESIMPULAN DAN SARAN .....</b>	<b>45</b>
5.1 Kesimpulan.....	45
5.2 Saran.....	46
<b>DAFTAR PUSTAKA.....</b>	<b>47</b>
<b>LAMPIRAN.....</b>	<b>49</b>



## DAFTAR GAMBAR

<b>Gambar 2.1</b> Table ASCII .....	8
<b>Gambar 2.2</b> Skema Algoritma SHA-256.....	11
<b>Gambar 3.1</b> Skema Fungsi Hash .....	19
<b>Gambar 3.2</b> Skema Enkripsi dan Dekripsi RSA.....	19
<b>Gambar 3.3</b> Skema Tanda Tangan Digital .....	20
<b>Gambar 3.4</b> Skema Pengembangan Model.....	21
<b>Gambar 3.5</b> Rancangan Tampilan Halaman Home .....	25
<b>Gambar 3.6</b> Rancangan Tampilan Halaman Registrasi Pemilih.....	25
<b>Gambar 3.7</b> Rancangan Tampilan Halaman Voting.....	26
<b>Gambar 3.8</b> Rancangan Tampilan Halaman Validasi .....	26
<b>Gambar 3.9</b> Rancangan Tampilan Hasil Pemilihan .....	26
<b>Gambar 3.10</b> Rancangan Tampilan Unggah Data Pemilih dan Panitia .....	27
<b>Gambar 3.11</b> Rancangan Tampilan Registrasi Panitia.....	27
<b>Gambar 4.1</b> Skema Aplikasi <i>E-Voting</i> Menggunakan Algoritma RSA dan SHA-256.....	30
<b>Gambar 4.2</b> Tampilan Halaman Admin .....	35
<b>Gambar 4.3</b> Tampilan <i>Alert</i> User Sudah Ditambahkan .....	35
<b>Gambar 4.4</b> Tampilan Halaman Register Pemilih .....	36
<b>Gambar 4.5</b> Tampilan Halaman Voting .....	37
<b>Gambar 4.6</b> Tampilan <i>Alert</i> Pemilih Sudah Melakukan Pemilihan.....	37
<b>Gambar 4.7</b> Tampilan Halaman Register Panitia .....	38
<b>Gambar 4.8</b> Tampilan Halaman Hasil Voting.....	38
<b>Gambar 4.9</b> Proses Registrasi Pemilih yang Sudah Terdaftar .....	40
<b>Gambar 4.10</b> Proses Registrasi Pemilih yang Belum Terdaftar .....	40
<b>Gambar 4.11</b> Proses Registrasi Pemilih yang Sudah Melakukan Pemilihan.....	41
<b>Gambar 4.12</b> Proses Registrasi Panitia yang Sudah Terdaftar .....	42
<b>Gambar 4.13</b> Proses Registrasi Panitia yang Belum Terdaftar.....	42
<b>Gambar 4.14</b> Proses Autentikasi.....	43

## DAFTAR TABEL

<b>Tabel 2.1</b> Nilai Awal Variabel SHA-256.....	12
<b>Tabel 3.1</b> Enkripsi dan Dekripsi RSA .....	24

## DAFTAR PUSTAKA

- Álvarez-Acebal, N. (2021). From *Javascript* to React. js: Best Practices for Migration.
- Burton, D. (2010). EBOOK: Elementary Number Theory. Edisi ke tujuh .McGraw Hill. Americas, New York
- Darmawan, I., Nurhandjati, N., & Kartini, E. (2014). Memahami E-voting: Berkaca dari Pengalaman Negara-negara Lain dan Jembrana (Bali). Yayasan Pustaka Obor Indonesia.
- Dinku, Z. (2022). React. js vs. Next. js.
- Fikriansyah, I. (2021). Program Aplikasi E-Voting Menggunakan Algoritma El Gamal dan SHA 256.
- Haverbeke, M. (2018). Eloquent *javascript: A modern introduction to programming*. No Starch Press.
- Istiqamah, N., & Subiyanto, S. (2016). Sistem Keamanan E-Voting Menggunakan Fungsi Hash dan Algoritma One Time Pad. *Edu Komputika Journal*, 3(1), 11-11.
- Kumar, S., & Walia, E. (2011). Analysis of electronic voting system in various countries. *International Journal on Computer Science and Engineering*, 3(5), 1825-1830.
- Maryanto, B. (2008). Penggunaan Fungsi Hash Satu-Arah Untuk Enkripsi Data. *Media Informatika*, 7(3), 138-146.
- Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography. CRC press.
- Menezes, A. V. (1996). Handbook of Applied Cryptography. CRC Press.
- Munir, R. (2004). Teori bilangan (Number Theory). Departemen Teknik informatika ITB.
- Munir, R. (2006). Kriptografi. Informatika, Bandung.
- Munir, R. (2010). Matematika Diskrit. Edisi keempat. Informatika Bandung, Bandung
- Munir, R. (2011). Algoritma dan Pemrograman dalam bahasa Pascal dan C. Edisi ketiga. Informatika, Bandung.

- Panjaitan, Z., Ginting, E. F., & Yusnidah, Y. (2020). Modifikasi SHA-256 dengan Algoritma Hill Cipher untuk Pengamanan Fungsi Hash dari Upaya Decode Hash. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, 19(1), 53-61.
- Ridwan, M., & Arifin, Z. (2016). Rancang bangun e-voting dengan menggunakan keamanan algoritma Rivest Shamir Adleman (RSA) berbasis web (studi kasus: pemilihan ketua BEM FMIPA).
- Risnanto, S. (2017). Aplikasi Pemungutan Suara Elektronik/E-voting Menggunakan Teknologi Short Message Service & At Command. *Teknik Informatika Vol. 10 No. 1*.
- Rokhman, A. (2011, July). Prospek dan tantangan penerapan e-voting di Indonesia. In *Seminar Nasional Peran Negara dan Masyarakat dalam Pembangunan Demokrasi dan Masyarakat Madani di Indonesia (Vol. 7, pp. 1-11)*.
- Stinson, D. R. (2005). *Cryptography: theory and practice*. Third Edition. Chapman and Hall/CRC.