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 Algoritm-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 Algoritm-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

Universitas Pendidikan Indonesia
Agustus 2004

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 dikontruksi 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 keamaanan 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

DAFTAR GAMBAR

DAFTAR TABEL

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.