ABSTRAK

IMPLEMENTASI ALGORITMA RSA (*Rivest Shamir Adleman*) UNTUK KEAMANAN SISTEM E-VOTING PEMILIHAN KEPALA DESA BERBASIS WEB

Oleh:

Azhar Zahid Misbahuddin

1197050022

Sistem pemilihan kepala desa (Pilkades) secara konvensional masih memiliki berbagai kelemahan, seperti potensi manipulasi suara, pemilih ganda, serta lambatnya proses penghitungan suara. Oleh karena itu, diperlukan solusi berbasis teknologi untuk meningkatkan transparansi dan keamanan. Penelitian ini bertujuan untuk mengembangkan sistem *e-voting* berbasis *web* yang aman dengan menerapkan algoritma kriptografi RSA guna menjaga kerahasiaan suara pemilih. Pengembangan sistem dilakukan menggunakan metode *Prototyping* Model, bahasa pemrograman Python (Flask), dan *database* SQLite. Algoritma RSA diterapkan dalam dua mode: demo (bilangan prima kecil, e = 7) dan nyata (bilangan prima 512-bit, e = 65537). Setiap suara diberi *padding* acak sebelum dienkripsi agar hasil enkripsi berbeda meskipun pilihan kandidat sama. Hasil pengujian menunjukkan bahwa sistem berhasil menghasilkan *ciphertext* yang unik, namun tetap dapat didekripsi secara akurat. *Log* proses RSA ditampilkan secara *real-time* di terminal untuk memudahkan verifikasi. Sistem juga menampilkan hasil pemilu dalam bentuk grafik dan membedakan hak akses admin dan pemilih. Dengan demikian, implementasi algoritma RSA terbukti efektif dalam menjamin keamanan dan kerahasiaan suara dalam sistem *e-voting* Pilkades berbasis *web*.

Kata Kunci: *e-voting*, RSA, keamanan data, Pilkades, Flask

ABSTRACT

Implementation of RSA Algorithm (Rivest Shamir Adleman) for Security in a Web-Based Village Head E-Voting System

By:

Azhar Zahid Misbahuddin

1197050022

Conventional village head election systems (Pilkades) often face various vulnerabilities such as vote manipulation, duplicate voters, and slow vote counting. Therefore, a technology-based solution is needed to improve transparency and security. This research aims to develop a secure web-based e-voting system by implementing the RSA (Rivest Shamir Adleman) cryptographic algorithm to ensure the confidentiality of voter choices. The system is developed using the Prototyping Model methodology, with Python (Flask) as the programming language and SQLite as the database. RSA is applied in two modes: demo (using small prime numbers with e = 7) and real (using 512-bit primes with e = 65537). Each vote is padded with two random digits before encryption to ensure that ciphertexts are unique, even when the chosen candidate is the same. Test results show that the system successfully produces different ciphertexts while maintaining accurate decryption. Real-time RSA logs are displayed in the terminal for verification purposes. The system also presents election results in graphical form and separates admin and voter access. Thus, the RSA algorithm proves effective in securing voter privacy in a web-based e-voting system for Pilkades.

Keywords: *e-voting, RSA, data security, Pilkades, Flask*