DESAIN DAN IMPLEMENTASI SISTEM KEAMANAN E-VOTING MENGGUNAKAN FUNGSI HASH DAN ALGORITMA ONE TIME PAD (STUDI KASUS: DESA PAYA PERUPUK KECAMATAN TANJUNG PURA KABUPATEN LANGKAT)

ABSTRAK

Pemungutan suara elektronik adalah proses pemilihan umum yang dilakukan secara elektronik. Oleh karena itu, untuk menjaga integritas proses demokrasi, penting untuk memastikan bahwa sistem pemungutan suara elektronik memenuhi standar keamanan dan privasi yang ketat. Maka dari itu penulisan skripsi ini bertujuan untuk mengembangkan sistem keamanan pemungutan suara elektronik untuk pemilihan kepala desa di Desa Paya Perupuk Kecamatan Tanjung Pura dengan menerapkan algotritma SHA 256 dan OTP. Keamanan sistem pemungutan suara elektronik yang dicapai harus memenuhi Lima komponen keamanan data antara lain kerahasiaan, otentikasi, integritas, ketersediaan, dan non-penyangkalan. Penerapan Sistem keamanan dalam proses pemungutan suara elektronik dilakukan dengan mengenkripsi hasil pemungutan suara yang disusun dalam bentuk plaintext. Sedangkan tahapan enkripsi dibagi menjadi dua, di mana tahap yang pertama menggunakan SHA-256, untuk melakukan hash pada plaintext. Tahapan yang digunakan algoritma hash dalam melakukan enkripsi data meliputi ketahanan, pengubahan plaintext, serta resistensi tabrakan. Hal tersebut memastikan integritas data maupun file yang bakal dikirimkan ke server penerima, selanjutnya disimpan dalam database. Selanjutnya Pada tahap kedua dilakukan proses keamanan menggunakan algoritma OTP. Pada algoritma digunakan kunci sepanjang plaintextnya dan bit kunci akan dibangkitkan secara acak. Ketika hasil dekripsi algoritma OTP sampai di server, maka di-hash menggunakan SHA-256. Nilai hash masing masing tahap ini selanjutnya dilihat perbedaannya. Jika nilainya sama maka hasil pemungutan suara dianggap valid dan aman dari serangan saat proses pengiriman ke server. Penelitian ini menunjukkan bahwa sistem yang dirancang dapat mengolah data dan memberikan

informasi tentang jumlah hasil pemungutan suara. Sedangkan dari segi keamanannya, sistem yang dirancang terbukti unggul karena aman dari serangan.
Kata Kunci : *E-voting, Algoritma one time pad, fungsi Hash SHA 256*

DESAIN DAN IMPLEMENTASI SISTEM KEAMANAN E-VOTING MENGGUNAKAN FUNGSI HASH DAN ALGORITMA ONE TIME PAD (STUDI KASUS: DESA PAYA PERUPUK KECAMATAN TANJUNG PURA KABUPATEN LANGKAT)

ABSTRACT

Electronic voting is a general election process that is carried out electronically. Therefore, to maintain the integrity of the democratic process, it is important to ensure that electronic voting systems meet stringent security and privacy standards. Therefore, the aim of writing this thesis is to develop an electronic voting security system for village head elections in Paya Perupuk Village, Tanjung Pura District by applying the SHA 256 and OTP algorithms. The security of an electronic voting system that is achieved must meet five data security components, including confidentiality, authentication, integrity, availability and non-repudiation. The implementation of the security system in the electronic voting process is carried out by encrypting the voting results which are compiled in plaintext form. Meanwhile, the encryption stage is divided into two, where the first stage uses SHA-256 to hash the plaintext. The stages used by the hash algorithm in encrypting data include resistance, plaintext change, and collision resistance. This ensures the integrity of the data and files that will be sent to the recipient server, then stored in the database. Next, in the second stage, a security process is carried out using the OTP algorithm. The algorithm uses a key along the plaintext and the key bits are generated randomly. When the OTP algorithm decryption results arrive at the server, they are hashed using SHA-256. The hash value for each stage is then seen for the differences. If the values are the same then the voting results are considered valid and safe from attacks during the sending process to the server. This research shows that the system designed can process data and provide information about the number of voting results. Meanwhile, in terms of security, the designed system has proven to be superior because it is safe from attacks.

Keywords: *E-voting, one time pad algorithm, SHA 256 Hash function*.