INTISARI

IMPLEMENTASI ENKRIPSI HOMOMORFIK RSA TERMODIFIKASI UNTUK SISTEM *ELECTRONIC VOTING*

Oleh

Ichsanul Akbar
16/395742/PA/17318

Salah satu hal di Indonesia yang sampai sekarang masih belum sepenuhnya menggunakan teknologi dalam pelaksanaannya adalah proses pemilihan umum. Proses pemilihan dan perhitungan hasil masih dilakukan secara manual, sehingga membutuhkan waktu yang lama. Untuk mengatasi hal tersebut, diperlukan sistem pemilihan yang lebih memanfaatkan penggunaan teknologi dalam proses pemilihannya, yaitu *e-voting*. Akan tetapi masih ada pihak yang meragukan sistem *e-voting* dari keamanan data pemilihannya.

Pada penelitian ini akan dilakukan perancangan sebuah prototipe sistem *e-voting* dengan menggunakan enkripsi homomorfik berbasis RSA termodifikasi. Enkripsi yang bersifat homomorfik dirancang agar data pemilihan dapat diproses dalam keadaan terenkripsi, dan terlindungi dari pembocoran data. Sistem yang dirancang merupakan sistem yang berbasis *website* yang dibangun menggunakan bahasa pemrograman *python* dan basis data SQLite. *Website* dijalankan didalam *server* yang memiliki sistem operasi Linux distro Ubuntu 18.04 serta memiliki 4 vCPU dan 16GiB RAM. Setelah pembangunan prototipe sistem, dilakukan evaluasi berupa akurasi hasil akhir dan analisis *security requirements* milik sistem.

Dari hasil pengujian, didapatkan bahwa enkripsi homomorfik diimplementasikan dengan benar, terbukti dari kebenaran hasil voting setelah dilakukan dekripsi. Selain itu, sistem juga memenuhi *requirement eligibility*, *unreusability*, *verifiability*, *tally correctness*, *uncoerability*, *auditability*, *fairness*, *efficiency* dan *integrity*.

Kata-kata kunci : e-voting; RSA; Modified RSA; Cryptography; Homomorphic; Encryption;

ABSTRACT

IMPLEMENTATION OF MODIFIED RSA FOR ELECTRONIC VOTING SYSTEM

By

Ichsanul Akbar
16/395742/PA/17318

One of the things that Indonesia have not make use of the technology is an election event. The manual voting process and manual calculation which will take a long time still needs to be fixed. Therefore, a more technology based voting system is needed, which is an electronic voting system. However, there are multiple parties that still doubting the security of the voting data in e-voting system.

In this study, a prototype of e-voting system thats using a homomorphic property of Modified RSA encryption algorithm is designed. Homomorphic encryption is used so the system can process voting data while still in an encrypted state, and protects the data from security breach. The designed system is a website based application that was built using python programming language and SQLite database system. The website is running on a server with Linux Ubuntu 18.04 as the operating system, with 4 vCPUs and 16 GiB RAM. After the system prototype is built, an evaluation about the system's final result's accuracy and security requirements analysis is done.

From the results of the evaluation, this system has implemented homomorphic encryption correctly, proven by the accurate result after the voting data is decrypted and also fulfills security requirements such as eligibility, unreusability, verifiability, tally correctness, uncoerability, auditability, fairness, efficiency and integrity.

Keywords : e-voting; RSA; Modified RSA; Cryptography; Homomorphic; Encryption;