ABSTRAK

Otorisasi User Menggunakan Algoritma *Rivest Shamir Adleman* dan *Advanced Encryption Standard* Pada *Database Server* Advokathan

Oleh: Rifki Mohammad Idrus

Pembimbing I: Ichsan Taufik, ST., MT.

Pembimbing II: Faiz M. Kaffah, MT.

Keamanan dalam sistem informasi merupakan salah satu hal penting karena semakin berkembangnya teknologi maka semakin besar kejahatan dunia maya terkait pencurian data. Oleh karena itu dibutuhkan suatu keamanan sistem informasi yang menerapkan algoritma dengan tingkat keamanan yang tinggi. Diantara algoritma yang handal adalah algoritma RSA dan AES. Algoritma RSA ini termasuk algoritma *asimetris* dimana kunci publik digunakan pada saat enkripsi dan kunci pribadi digunakan saat dekripsi. Kehandalan dari algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi bilangan prima. Sedangkan algoritma AES tingkat kesulitannya terletak pada panjang kunci yang digunakan pada saat enkripsi. Pengujian dilakukan terhadap 10 email dan password yang diimplementasikan kedalam sistem otorisasi user. Ketika pengguna melakukan register maka password yang diinputkan akan dienkripsi menggunakan algoritma RSA, hasil enkripsi RSA tersebut dienkripsi ulang menggunakan algoritma AES sehingga data yang disimpan dalam bentuk *ciphertext* AES. Hasil yang didapatkan adalah password pengguna yang sudah dienkripsi dan disimpan dalam *database*.

Kata Kunci: Otorisasi, Kriptografi, *Simetris*, *Asimetris*, RSA, AES

ABSTACT

User Authorization With Rivest Shamir Adleman and Advanced Encryption Standard Algorithm on Advokathan Database Server

By: Rifki Mohammad Idrus

Supervisor I: Ichsan Taufik, ST., MT.

Supervisor II: Faiz M. Kaffah, MT.

Security is one of the important aspects in information systems because the more technology develops, the greater the cyber crime related to data theft. Therefore we need an information system security that applies an algorithm with a high level of security. Among the reliable algorithms are the RSA and AES algorithms. This RSA algorithm includes an asymmetric algorithm where the public key is used at the time of encryption and the private key is used at the time of decryption. The reliability of the RSA algorithm lies in the level of difficulty in factoring non-prime numbers into prime numbers. Meanwhile, the difficulty level of AES algorithm lies in the length of the key used at the time of encryption. Testing is done on 10 emails and passwords which are implemented into the user authorization system. When the user registers, the input password will be encrypted using the RSA algorithm, the results of the RSA encryption are re-encrypted using the AES algorithm so that the data stored is in the form of AES ciphertext. The result is that the user's password has been encrypted and stored in the database.

Keywords: Authorization, Cryptography, Symmetric, Asymmetric, RSA, AES