IMPLEMENTASI ALGORITMA *SYMETRIC KEY ADVANCED ENCRYPTION STANDARD (*AES) DAN BLOWFISH MENGGUNAKAN OTENTIKASI GENERATE *ONE TIME PASSWORD* (OTP) PADA KEAMANAN DATA *FILE*

ABSTRAK

Penelitian ini bertujuan untuk menghasilkan kerahasiaan data file data dan otentikasi terhadap pengambilan data yang dilakukan oleh user. Kemanan terhadap kerahasiaan data sangat penting untuk menjaga keaslian dari data tersebut, untuk menjaga keasliannya data tersebut akan dienkripsi menggunakan algoritma blowfish. Kemudian untuk mengambil data tersebut akan dilakukan verifikasi dengan menggunakan *One-Time-Password* berupa kode otentikasi yang diberikan kepada user. Kode otentikasi ini dihasilkan dari hasil *generate* kombinasi *lowercase*, *uppercase*, dan *number*. Kemudian, kode tersebut akan dienkripsi menggunakan algoritma kriptografi *Advanced Encryption Standard* yang ekspansi kuncinya didapat dari hasil *hashing* algoritma SHA-256, kode otentikasi yang dihasilkan hanya dapat digunakan satu kali dalam waktu yang terbatas. Setelah proses *hashing* dilakukan, langkah selanjutnya dilakukan uji coba dengan menghitung waktu enkripsi dan dekripsi terhadap algoritma blowfish terhadap data file**,** kemudian *ciphertext* dari algoritma blowfish dan kunci dari hasil *hashing* dilakukan pengujian dengan uji *Randomness Test*, dari 5 data file yang menjadi uji coba *ciphertext* algortima blowfish mampu melewati kelima tes acak dalam *randomness test* dengan hasil yang sangat baik, dan kunci AES-256 bit mampu melewati kelima tes acak dasar dalam *Randomness Test* dengan hasil yang sangat baik.

Kata Kunci—*Advanced Encrytopn Standard*; Blowfish; SHA-256; *One-Time-Password*; Hashing

IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES) AND BLOWFISH ALGORITHMS USING AUTHENTICATION ONE-TIME-PASSWORD (OTP) ON FILE DATA SECURITY

ABSTRACT

study aims to implement AES and Blowfish algorithm by using OTP verification in data security, knowing the process of data capture with authentication that implements Advanced Encryption Standard and One-time Password algorithm, knowing result of AES-256 algorithm combined with SHA-256 as authentication data retrieval, and result of application of Blowfish algorithm to data confidentiality and randomness testing to ciphertext encryption result. Security of data confidentiality is very important to maintain the authenticity of the data, to keep the authenticity of the data will be encrypted using blowfish algorithm. Then to retrieve the data will be verified by using One-Time-Password in the form of authentication code given to the user. This authentication code results from the resulting lowercase, uppercase, and number combination. Then, the code will be encrypted using Advanced Encryption Standard cryptographic algorithm whose key expansion is obtained from SHA-256 hashing algorithm, the generated authentication code can only be used once for a limited time. After the hashing process is done, the next step to test by counting the time of encryption and decryption to blowfish algorithm to data file, then ciphertext of blowfish algorithm and key from hashing result is tested by Randomness Test, from 5 data file become test of ciphertext algortima blowfish was able to pass all five random tests in randomness tests with excellent results, and the AES-256 bit key was able to pass the five basic random tests in a randomness test with excellent results.

Keywords—*Advanced Encrytopn Standard; Blowfish; SHA-256; One-Time-Password; Hashing*