IMPLEMENTASI KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES) SEBAGAI SISTEM KEAMANAN DATA PADA ARSIP DESA

ANGGITA DIAN BERLIANTI
Program Studi Informatika, Fakultas Sains dan Teknologi
Universitas Teknologi Yogyakarta
Jl. Ringroad Utara Jombor Sleman Yogyakarta
E-mail: anggitadianb@gamil.com

ABSTRAK

Pengelolaan arsip surat pada kantor desa belum sepenuhnya sesuai prosedur dan belum terstruktur. Selain itu, proses penerimaan hingga penyimpanan surat masih dilakukan secara manual. Dalam penyimpanan surat masuk maupun surat keluar masih berbentuk hard copy kemudian surat disimpan pada rak arsip. Untuk pencatatan surat dilakukan pada buku agenda. Selain itu untuk melakukan pencarian arsip surat membutuhkan waktu yang lama karena harus membuka terlebih dahulu kumpulan arsip satu per satu, sehingga ini kurang efisien dan data penting rentan bocor dan di salah gunakan oleh orang yang tidak bertanggung jawab. Hal ini masih kurang efektif karena membutuhkan waktu yang cukup lama dalam mengolah data dan kemungkinan buruk bisa terjadi jika data tersebut hilang atau rusak. Penelitian ini mengimplementasikan metode AES untuk keamanan data pada aplikasi arsip desa yang memberikan kemudahan dalam melakukan pengelolaan data surat masuk, surat keluar dan data desa. Sistem ini dibuat sesuai dengan kebutuhan pada sistem arsip desa dengan merubah sebuah data desa menjadi sebuah kode byte dengan cara enkripsi dekripsi, hasil penelitian telah dibuktikan bahwa isi file awal yang mengalami proses enkripsi, kemudian mengalami proses dekripsi, maka akan kembali seperti file awal semula jika memasukkan private key dengan benar.

Kata kunci: Keamanan Informasi, Arsip Desa, AES, Kriptografi.

IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES) CRYPTOGRAPHY AS A DATA SECURITY SYSTEM IN VILLAGE ARCHIVES

ABSTRACT

The management of the letter archives at the village office has not been entirely following procedures and has not been structured. In addition, receiving and storing letters is still done manually. In the storage of incoming and outgoing letters, they are still in hard copies, and then the letters are stored on archive racks. Letters are recorded in the agenda book. In addition, searching for mail archives takes a long time because they have to open a collection of archives one by one, which is less efficient, and essential data is prone to leaking and being misused by irresponsible people. This is still ineffective because it takes a long time to process data, and problems occur if they are lost or damaged. This study implements the AES method for data security in the village archive application, which provides convenience in managing incoming mail, outgoing mail, and village data. This system is made according to the requirements of the village archive system by converting village data into a byte code utilizing encryption and decryption. The study results have proven that the contents of the initial file that undergo the encryption process, then the decryption process, will return to the original file if you enter the private key correctly.

Keywords: Information Security, Village Archives, AES, Cryptography.