ABSTRACT

APPLICATION OF RSA (RIVEST SHAMIR ADLEMAN) ALGORITHM FOR CRIPTOGRAPHIC SYSTEM AUDIO MP3 FILE

By :
Ngakan Nyoman Diarse
1213001

The problem of data security is one of the important aspect of information technology. One solution that can be used to maintain data security is cryptography. Cryptography is a field of knowledge that use mathematical equations to perform encryption and decryption of data either by applying algorithms asymmetry such as the DSA (Digital Signature Algorithm), RSA, DH (Diffie-Hellman), ECC (Elliptic Curve Cryptography), and Cryptography Quantum. Of the many asymmetric algorithms are made, the most popular algorithm is the RSA algorithm. Security RSA algorithm lies in the difficulty of factoring large prime numbers are relative. To prove the security of the RSA algorithm is needed media as the data to be secured like the MP3 audio format. The MP3 format is one of the audio format most commonly used in the storage of audio data, because data is stored resemble the original data when recorded, and has a size that is not too large compared to other formats. Applications cryptographic system created in order to implement the RSA algorithm for encryption and decryption of MP3 audio files. The result is the application of a cryptographic system can encrypt the MP3 audio file can then decrypt back MP3 audio files that have been encrypted. MP3 audio files are encrypted still playable but his voice was not audible to the human ear so that the necessary application to decrypt the MP3 audio file to be played as before.

Keywords : Cryptographic System, RSA Algorithm, Audio MP3 File