

AN IMPLEMENTATION OF AN AUDIO ENCRYPTION SYSTEM USING REAL TIME AUDIO COMMUNICATION

Prepared by: Shashidharan Narayanasamy

ABSTRACT

In this project, a secure way of transmitting audio stream (speech) through networks is presented by implementing cryptography and digital signature. The purpose of this system is to encrypt the audio stream, and also to implement digital signature in exchanging the symmetric-key that will be used to encrypt and decrypt the audio stream. The ADPCM compression method is used to compress the audio stream to reduce the transmission time. Encryption to the audio stream is done using the RIJNDAEL algorithm. In implementing the digital signature, the MD5 hash function is used to produce the message digest for the symmetric-key cryptosystem is used to generate the public and private keys. This system was developed to overcome the limitations and also to improve the security services provided by current similar speech communication system.