Title of Project: TEXT ENCRYPTION

Cryptosystems are highly technical systems that provide security through secret encoding and have been an important part of the electronic information world for many years. Encryption and decryption are fundamental requirements of every Application.Therefore, the Java platform provides strong support for encryption and decryption through its Java Cryptographic Extension (JCE) framework which implements the standard cryptographic algorithms such as AES, DES and RSA.

Encryption, a process of encoding a message. Encryption Algorithms are of two types - symmetric-key algorithm and asymmetric-key Algorithm. For symmetric-key algorithm, the same cryptographic key is used for both encryption and decryption, in comparison to asymmetric-key algorithm symmetric-key algorithm like AES is usually high speed and low RAM requirements, but because it's the same key for both encryption and decryption, it's a big problem of key transport from encryption side (sender) to decryption side (receiver). For asymmetric-key algorithm, it requires two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt text or to create a digital signature.

This Projects is about Text Encryption using the *Advanced Encryption Standard (AES)* algorithm. Here, we will generate a random AES key is generated to encrypt files with key size (Standard Key size of AES which is 256 bits). The AES key is encrypted to a file using the RSA cipher where the RSA public key is assumed to be stored in a file.