**EXPERIMENT NO – 10**

**AIM**: Implementation of Cryptography Lab.

**THEORY**:

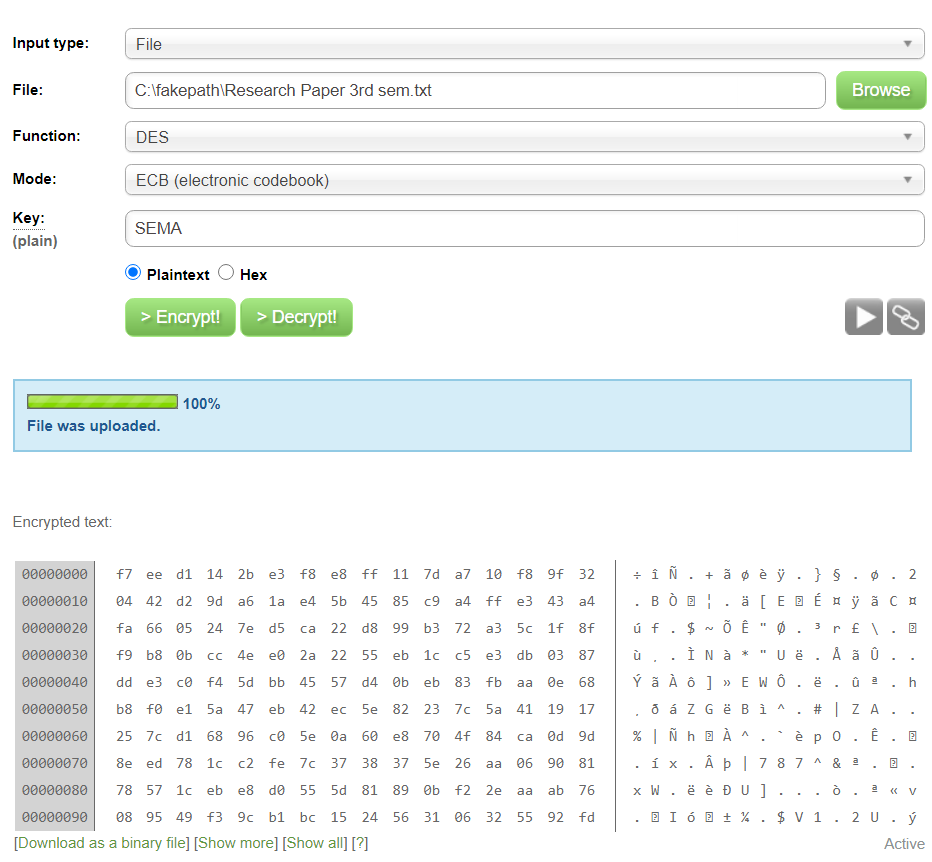
Symmetric key cryptography is any cryptographic algorithm that is based on a shared key that is used to encrypt or decrypt text/cyphertext, in contract to asymmetric key cryptography, where the encryption and decryption keys are different. The keys may be identical, or there may be a simple transformation to go between the two keys. Symmetric-key encryption can use either stream ciphers or block ciphers.

1.Stream Cipher encrypt the digits (typically bytes), or letters (in substitution ciphers) of a message one at a time.

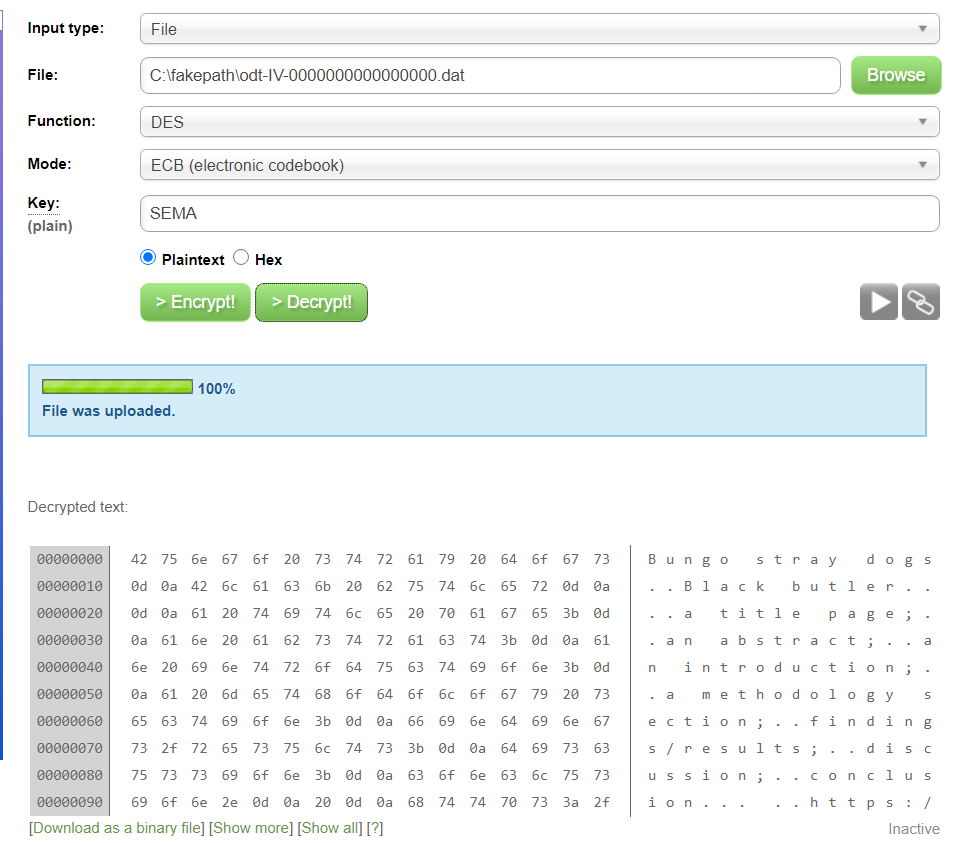
2.Block Cipher take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size.

Implementation of DES: Disk Encryption System

**Encryption:**



**Decryption:**



Asymmetric cryptography is a branch of cryptography where a secret key can be divided into two parts, a public key and a private key. The public key can be given to anyone, trusted or not, while the private key must be kept secret (just like the key in symmetric cryptography).

Asymmetric cryptography has two primary use cases: authentication and confidentiality. Using asymmetric cryptography, messages can be signed with a private key, and then anyone with the public key is able to verify that the message was created by someone possessing the corresponding private key.

Implementation of AES: Advanced Encryption Standard

Encryption and Decryption:

