Assignment1

Explanation of encryption algorithm:

The encryption script in Encrypt.py is based on **differential XORing** of bit blocks. The plaintext file is scanned in blocks of **64** bits and the output produced for each block is made a function of the output for the previous block.

The encryption script requires a **key** and a **passphrase.**

Passphrase is used as **initialization vector (IV)**.

The plaintext file is scanned in bit blocks, with each block being of size BLOCKSIZE (here BLOCKSIZE = 64).

Since the size of plaintext in bits may not be an integral multiple of BLOCKSIZE, appropriate number of 0 bytes are appended to the last block to make its size same as BLOCKSIZE.

Each bit block read from the message file is first XORed with the key and then with the output produced for the previous bit block.

Let bi represent blocks of plaintext and Bi represent corresponding blocks of ciphertext.

Then:

B1 = b1 **xor** key **xor** IV
B2 = b2 **xor** key **xor** B1 = b2 **xor** b1 **xor** key **xor** IV
B3 = b3 **xor** key **xor** B2 = b3 **xor** b2 **xor** b1 **xor** key **xor** IV
B4 = b4 **xor** key **xor** B3 = b4 **xor** b3 **xor** b2 **xor** b1 **xor** key **xor** IV
B5 = b5 **xor** key **xor** B4 = b5 **xor** b4 **xor** b3 **xor** b2 **xor** b1 **xor** key **xor** IV