Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

Name: Swasti Jain
Sem: 5, Branch: IT, Batch: 2

Experiment No. : 5

Date: 16/09/2022

Title: Block cipher modes of operation using AES or DES

Problem Definition: Compare different block cipher modes of operation by encrypting a long message "Because of you, my darling, I have known how it feels actually to care and cherish someone more than anything one can ever think of in this world. I have the chance to experience the most beautiful feeling of knowing that there will always be a person who will never give up on me and always cherish and care for me no matter what happens" using online AES or DES cryptosystem.

Pre-requisite: AES & DES

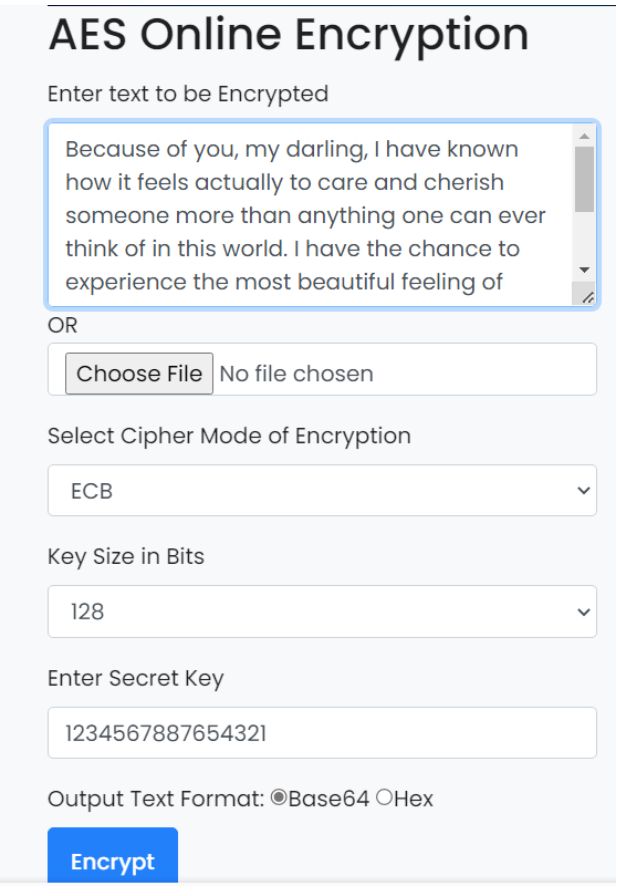
Theory:

Encryption algorithms are divided into two categories based on the input type, as a block cipher and stream cipher. Block cipher is an encryption algorithm that takes a fixed size of input, say b bits and produces a ciphertext of b bits again. If the input is larger than b bits it can be divided further. For different applications and uses, there are several modes of operations for a block cipher.

1) Electronic Code Book (ECB) – Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in the form of blocks of encrypted ciphertext.
2) Cipher Block Chaining – Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, the previous cipher block is given as input to the next encryption algorithm after XOR with the original plaintext block.

3) Cipher Feedback Mode (CFB) – In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first, an initial vector IV is used for first encryption and output bits are divided as a set of s and b-s bits.The left-hand side s bits are selected along with plaintext bits to which an XOR operation is applied. The result is given as input to a shift register having b-s bits to lhs,s bits to rhs and the process continues.
4) Output Feedback Mode – The output feedback mode follows nearly the same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output. In this output feedback mode, all bits of the block are sent instead of sending selected s bits. The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases the dependency or relationship of the cipher on the plaintext.
5) Counter Mode – The Counter Mode or CTR is a simple counter-based block cipher implementation. Every time a counter-initiated value is encrypted and given as input to XOR with plaintext which results in a ciphertext block. The CTR mode is independent of feedback use and thus can be implemented in parallel.

Procedure/ Algorithm :



AES Encrypted Output:

AybbWyjzFUT7lZi93M92LQEFOhkMtaUVzfEwJ4
DjQ/Tz+CJEV7am5LTgJybAfgvO+ovYo0/3u7
6KVZoJYPMEWpI27XfYL/s9o0JehqJrVah5Mn
bM2k4mHLlCcnrX7bwu/d1aq+rnTOUz6F8kvM
Nee193pw+DQBdrTfgmUa9KN6SsQF5b+JTqS
t0pyhWXAte/PRM7i3O/jl5okaKgYGhN7z5A3lu
uqV1ylwBMZSrlUXZjw+bUtatnY+jzWxPwz3Kgp
bIAGfvzU0loMyyB/ggSMVsUMhTMpUE7hs9z3
X/5Hklg3tkuhUdqeRTBYvQ9g7joymYFf8+cOs
74vUUhlvpItqdEkppDkleVjuZ4YhW+7X2Bivrtl+
RI+k/qSliYcNpvNfNtbdVp9od5XAUGVAumtvb
G8lTVvNQw9Xi0Co43LPK2EY5wf9pi/lkxuUml
wmjlmi+Y/g8O9GHu159dQj19Uw==

DES Encryption

Input Content

Because of you, my darling, I have known how it
feels actually to care and cherish someone more than anything one can ever
think of in this world. I have the chance to experience the most beautiful
feeling of knowing that there will always be a person who will never give up
on me and always cherish and care for me no matter what happens

Mode	ECB	Padding	pkcs5padding	Password	12345678
In-Format	string	Out-Format	hex	Charset	UTF-8

Encrypt Decrypt Clear

Output Result

d55ae27719041ebca6decd16da3da451fd1ad4e7012aa91f3dea8b19bef90b021fb08d0f9735d58d7fe68cebb67aa5dc0fa8e3d4d25f4733e35ff2fd39ace21263338399c46495dc09569b02ac152f81ef95a78a0860d8dfa2c9f159ee
66f367852c652452ebffb7469e081d2b2122343786cddc1a1106e2b1d8ee5b071bf092b685835a96f0aaf842d6dabeb1fc654e4d556e07e128bddb78c2b5969aa612f10a0865df1821b374cfd7886354cec8d6158c7bb48ac110d818602
49a59f6af253e323c03fa94ced582033d8161761ed04abb56341728a7e29bac002ad60476a3ab16783435c26049e4839aa1af1bb87ad2c425cb7a2e2b6db2fa5c66257311a9ce9e5fdc29fd88eac024c8374d8fa0996696bc94ada31cd
6cb71a9f52e43b2edf80e914751ccf1b5accd508531c052f2ce27a74b1428e8b4419d32b4bdc268e7471b9bc4c4e7d60c3c3ca2a63172275a52e236ee484bb

2. Comparison between AES & DES

DES vs AES

	DES	AES
Date	1976	1999
Block size	64	128
Key length	56	128, 192, 256
Number of rounds	16	9,11,13
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but accept open public comment
Source	IBM, enhanced by NSA	Independent cryptographers

References :

1.https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a. pdf
2. https://www.geeksforgeeks.org/block-cipher-modes-of-operation/
3. https://web.cs.ucdavis.edu/~rogaway/papers/modes.pdf
4. https://www.youtube.com/watch?v=fgyfvRuhMvM.