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

Experiment No.: 5

Date: 16/09/2022

Name: Lavena Babu Roll No.:29

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.

Prerequisite :
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.

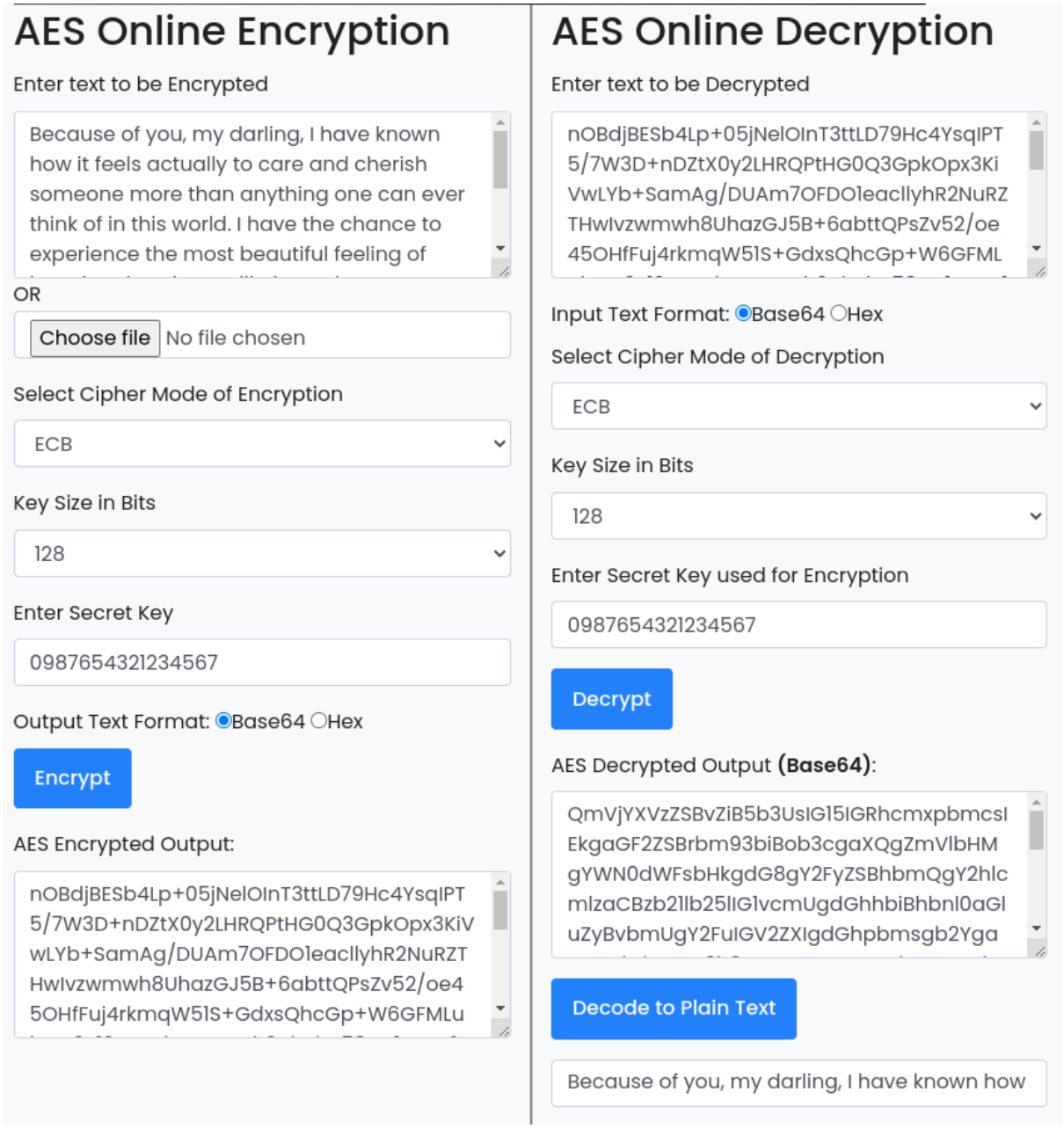
5. **Counter Mode –** The Counter Mode or CTR is a simple counter-based block cipher implementation. Every time a counter-initiated value is encrypted and given as input to XOR with plaintext which results in a ciphertext block. The CTR mode is independent of feedback use and thus can be implemented in parallel.

Procedure/ Algorithm :

AES Encryption:
Copy paste the text given in the problem definition in an online tool.
(Eg: https://www.devglan.com/online-tools/aes-encryption-decryption)
Select the Cipher mode of encryption to ECB (Electronic Code Book)
Select key size as 128 bits
Enter a secret key.
Output Text format: base 64
And click on Encrypt.

AES Decryption:
Next, copy the same AES Encrypted output and paste it in the text field provided for text to be decrypted.
Input text format is Base 64
Select Cipher mode of Decryption as ECB
Key size: 128 bits
In the Secret key field, enter the same secret key you used to encrypt the text.
Hit Decrypt and decode to Plain text.

Results : Online system snapshots:



Encrypted message:

```
nOBdjBESb4Lp+05jNelOInT3ttLD79Hc4YsqIPT5/7W3D+nDZtX0y2LHRQPtHG0Q3Gpk
Opx3KiVwLYb+SamAg/DUAm7OFDO1eacllyhR2NuRZTHwIvzwmwh8UhazGJ5B+6abtt
QPsZv52/oe45OHfFuj4rkmqW51S+GdxsQhcGp+W6GFMLubOp0y12BMLvjXWaVvUh2
VbvbB58sM1U4Z+1D3krdV4PcySvenxlhGPDYhoGV/nuyppMUjT9Cm3IP4315VgrvzqM
MRq3YSxZYgKYP9niYuh/2o4KqE6/ESaFosZv51KZ3KMXQno6iRwqEatJ0cHhV1G4Sgd
OV4mFa/7ev1GGDyjhmwkT7HqntZ7j9B2UbloNlmTU0cD82m/uzYqiWHIdjM5/zE0p7n/m
lqhV2lzOoeHM5Qf2+ienu27emcuX2SBFhg8b9F6foKzrflpeHJK6W8zHAIk0zmyn5GAz4C
IX2HbHJTh82/s8wDLSc2dB684NGuORKhM8Wai4CV
```

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.Online tool: https://www.devglan.com/online-tools/aes-encryption-decryption
2. Theory: 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