Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology
Experiment No. : 5

Name: Mohammad Zaid Ansari Roll No.: 03 Date: 14/09/22

Title : Block cipher modes of operation using AES or DES.

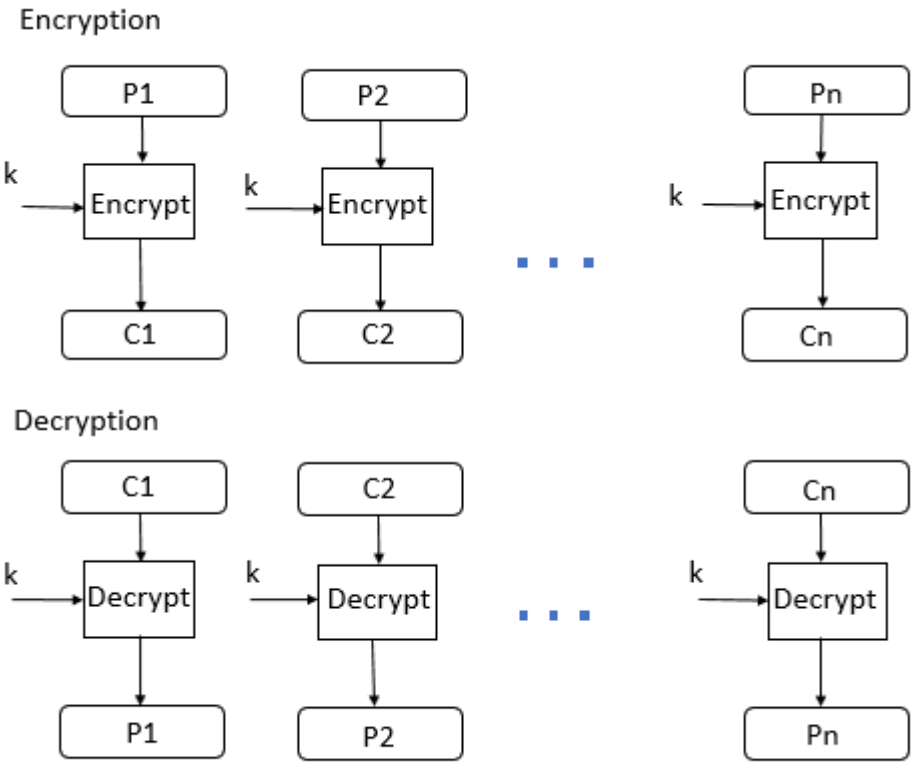
Problem Definition :

Compare different block cipher modes of operation by encrypting 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.

Theory and Algorithm :

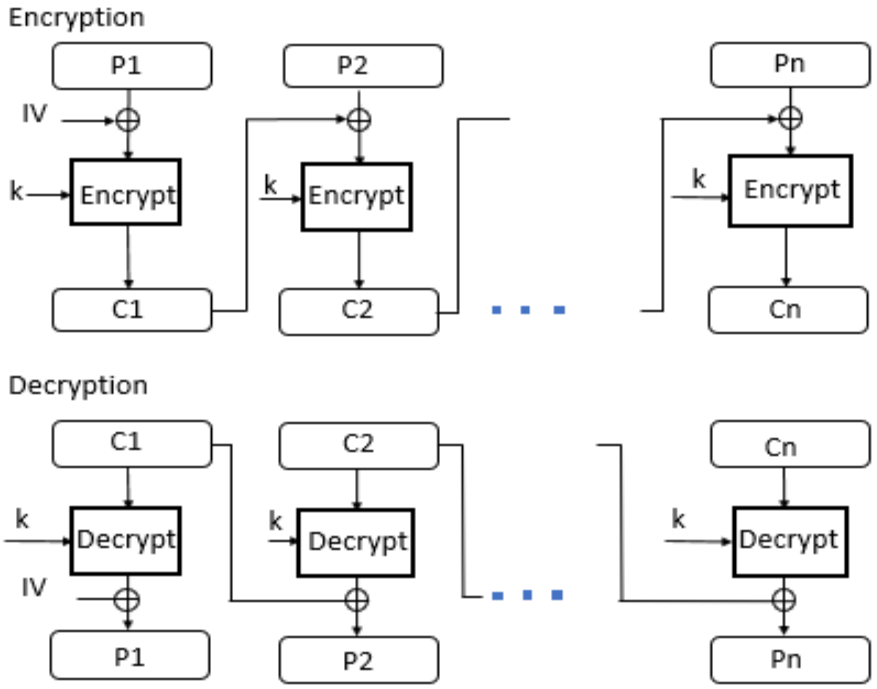
1. ECB mode

ECB mode stands for Electronic Code Block Mode. It is one of the simplest modes of operation. In this mode, the plain text is divided into a block where each block is 64 bits. Then each block is encrypted separately. The same key is used for the encryption of all blocks. Each block is encrypted using the key and makes the block of ciphertext.



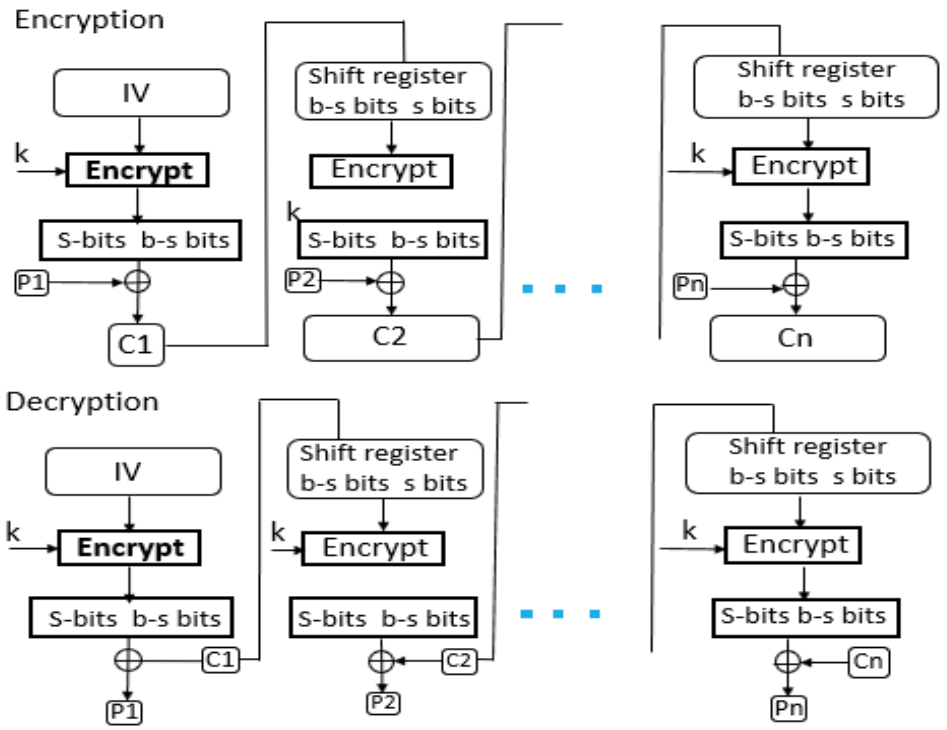
2. CBC Mode

CBC Mode stands for Cipher block Mode at the sender side; the plain text is divided into blocks. In this mode, IV(Initialization Vector) is used, which can be a random block of text. IV is used to make the ciphertext of each block unique.



3. CFB Mode

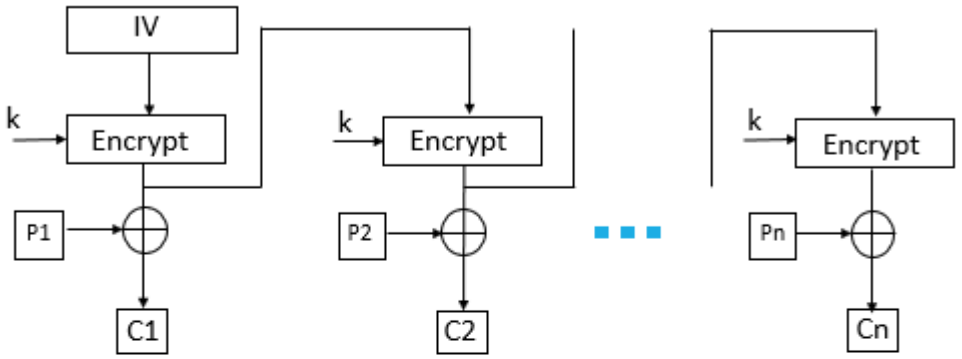
CFB mode stands for Cipher Feedback Mode. In this mode, the data is encrypted in the form of units where each unit is of 8 bits.



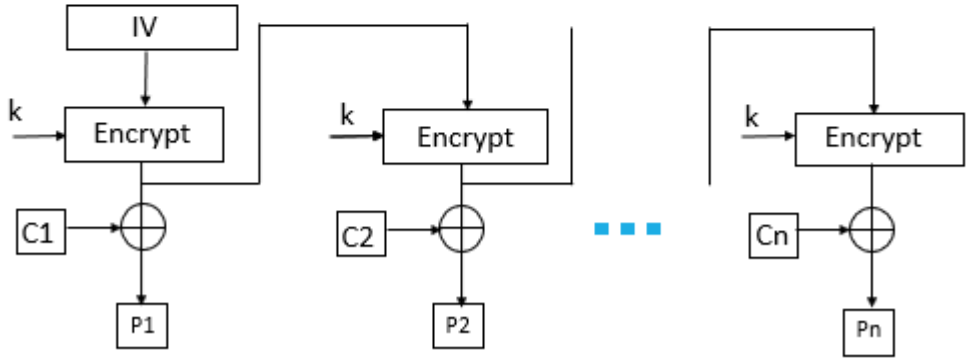
4. OFB mode

OFB Mode stands for output feedback Mode. OFB mode is similar to CDB mode; the only difference is in CFB, the ciphertext is used for the next stage of the encryption process, whereas in OFB, the output of the IV encryption is used for the next stage of the encryption process.

Encryption



Decryption

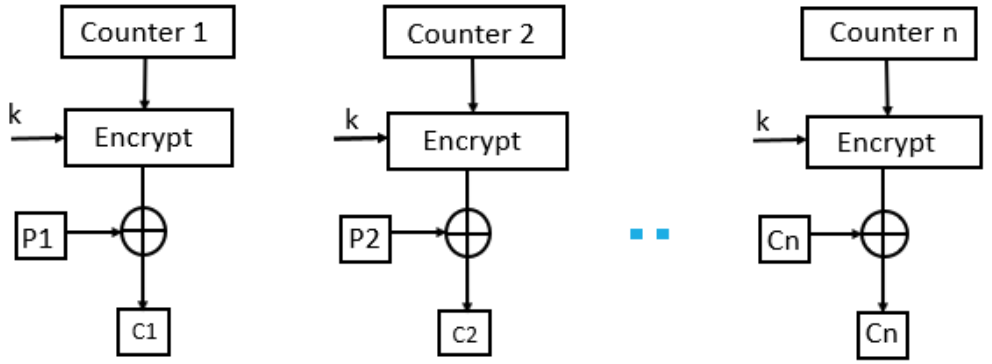


5. CTR Mode

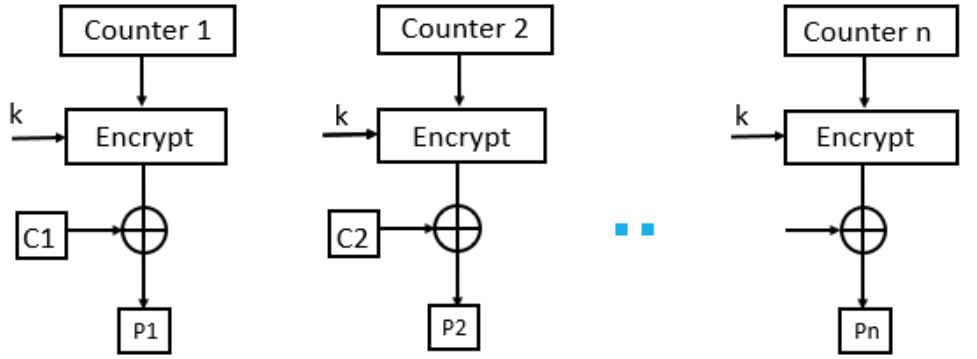
CTR Mode stands for counter mode. As the name is counter, it uses the sequence of numbers as an input for the algorithm. When the block is encrypted, to fill the next register next counter value is used.

Note: the counter value will be incremented by 1.

Encryption

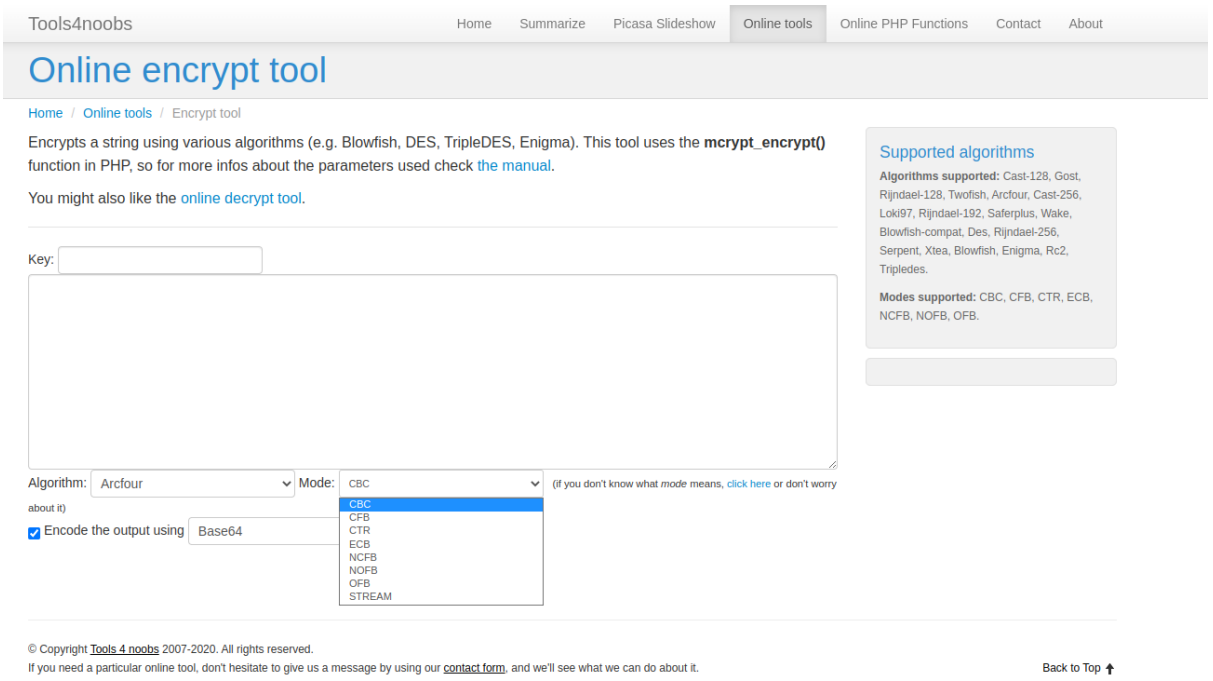


Decryption



Results :

Online system snapshots



Plain Text:

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

1. ECB:
   +aZ8YtgeTHHIaAzXn9qr1b148ivXZGZKU1Lvbj7tqkmGzhbMhU6kJCyJQ5pYududphIli3Dy+Lip93RJHa/S9LfPA5z2cmpZixGKeJtgYgPrG/oYZzz5OX7sSEwOv+6JI2fjiYEU5JD8dam/7rir8UeVj0iR/jymM535cPcdg0i8dSpOu1PLbQSiAmpms9/VjA7vsP56jWKiwZBBdM2+JcyMvmWpMzVTscUZIJvirDobTO4KamhYVYb14Q0jFrW5nVpP/tTweNwKiX5/CU9OQ6DJrxLA/LuDsEhIU6r8Ne44UWa84FaVFZ9FJmZ1wAFdf0WaekG9DnXG9E5Mm8TEmpm3UkkLHJiNGzcG5rRf5CQlxeBJvIk+7Hn+Lidoare9BGFPIZeYM2Xqn9qpHnYTSvNPQL0gBY3IX1yMH01Dh2OoNyVCgKgWkNBEs/3foPy48rP48nhGxek=
2. CBC:
   eNNnyZHW79FkSEOP9tHSjfE1p9l+Rvxu147OXu1JR5Ud5PUpFx0qbUdvgBYsP9IQJ6S7ukswYncb4gqckugWbx60WutoBAUzY+VhIc2hnlxt4ixk6mCaAH+sEgJtjkt7tzj3eGZrB78vCdJwA/ALVV1YJHtF0uCFi8wzxIJinfPyr9BFs+9FjjstCFSEj0oUFWgsI7nbggLRlwUq9M74VyM8KcNwNqb9wNT9uxo8/6KBsFUlf7mFyZ/KmUIEl2Ulg1zT7db0ezIMXCFBbiP1Ct4Np1+qXoeFC1uSMnBewP9X/t4H10iPh5eROHqHAqeMWMtB6fPOh0khKhYdQsKFm6+C58hyiyiXh+I+nWOArSA

aBqc3fPejhwDrbbi2azHnHfyHGMcKqXtXZgENEoC9DVHub9IR5XE42w9K+x8iev2knXTpdhqeenlslm1C81dqiozEfqa3J1I=

3. CFB:
   m8XfixnOFxQSSjyJRrTXdxsOq426EY1FrtudtX8bIlkqPmUv2H62ilUShD/ZdxEA2PcYSUPGIfrkaESCHe6mf19fquaqLky0Qg8wqisXDI3TNXbtZfZZ7Jd5vSthT6Wn+hD+5p2hVG2i5m6cArDWqKO6jqMyzgvdZVBWsWDJhjnQkLcG6t/azkyOS2Nh7thyaSqWfcqO7ZiAe99CVYySp14uYAs19WhU3qdR/oQkDSI6D6KogFMwARrnoGsVfIBLBlUEhPFmGWPRKmEaGQydsTnCooKq7QgSTruz9Zi2VChAgTJonghrLZ2Kj1INW1IAGM/hlM2qe5UNWKVc3Aj7XF7/k4BEPXNiqEnEyebRYJd8sOsd/P3oWBweEmE5oexuaBw9xjKamURDTEP7slcuUhWJRapsJomQ02qUgZKQtPFD0w7ZKI0vO8zwhPiAy/AoT7w=
4. OFB:
   m0bU5gtA8SZRc9MHAoIq+ShgNmb1M8scUiWiJrfSHEiBD6VckMZisiWHjves45TaAONkIv21uh/4ydbl4SJSJ8zFBnjaCKqIP+r1uaVEe+1ZX0rP4pIwEHYlnVVwzE9zCsn0caka9BuM+7lzskE6ntm7ASBCehiIRx2JxDzRLIYxJXMdX8EVk5yGVz2WNTNYrpJqT7gRP4nuf8C+dyq3JGRD2acQtsAKw6rDTM2AMoDkDT8y7mRKhGPMc+bD+YWcx4JyH562m6/VPwCZ1DEp2ZSShEgkTHz/0wuj/svLCeAcadCVlj6k4U5qF999/zSAStqB++HTWy1EIUZmfiYX1KfnkRoMZb3LSjUjbTQx7EwI6DGTGZ2N2LEgiQFY4uHrtM5u1utMZF7+uIJVvS2bWWJE2pXUUIsRH+YNiFbRBZpJFIxH8fl94apgzL+XAVmK/QA=
5. CTR:
   m9GxBBLvoSsMII0cmc94LksiZEEW0qif/qdKIUXbcj8I9Ptg1EYXs9YcJPxBFKzw21JmcPlfyFnNAwiYTQ+oHBPolHV3Afdti3Gwcn0cPGR7LbmbAH1OwZ4XPf/c8rw8MHMEzrUCd/7V9o56hwhkq2VOsSP7KS/BPo2VXeCMp2ib65TuZ9theuPmKpyIZsL4ESKhgt12A6YRVkHZaJBQItkTIzCu7p0AD7J9DCzVAs1k2at2pmswTik4dJsT4ckjybSQ1NS64hZj4iclKhI5E4lQxRCBf3cW+6SvGHd1kpGE3rrg38P4V4WUrVN80cHHAIZkB1uBhwxRpghIfCqdCllm1xY2TccMWu1P4VEaIJc17/q8fVshhkvadDCAWnZu7VFM+xZGDuMK39VKXTqNEgUL5H/5VQhd7E4CqswyMDOQ7kGs9t8BY8FWVFK/DQrL+Q=

Comparison:

Evaluation criteria	ECB	CBC	CTR	CCM	CC
Chain dependency	No	Yes	No	No	Yes
Error propagation	No	One block	No	No	One block
Authentication code	No	Yes	No	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes	Yes
Number of passes	One	One	One	Two	Two
Parallelism	Yes	No	Yes	No	Yes
implementing nonce	No	No	Could be	Yes	No, but could be in the counter
Message size	Any	Any	Any	Fixed	Any
Block cipher algorithm	Any	Any	Any	only with 128-bit block size algorithms	Any

ECB=electronic code book, CBC=cipher block chaining, CTR=counter, CCM=counter mode with the CBC-MAC mode, CC=counter chain.

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

Questions (Short, Long, MCQs) (optional) :

L1: Explain different Block cipher modes of operation.