In [ ]:
```
Practical No. : 04
Title : Write a Java/C/C++/Python program to implement AES algorithm.
Program Code with output
```

In [1]:
```
pip install PyCryptodome
```

```
Requirement already satisfied: PyCryptodome in c:\users\deshm\anaconda3\lib\s
ite-packages (3.17)
Note: you may need to restart the kernel to use updated packages.
```

In [2]:
```
from Crypto.Cipher import AES
from secrets import token_bytes
```

In [3]:
```
def encrypt(msg,key):

  cipher = AES.new(key,AES.MODE_EAX)

  nonce = cipher.nonce

  cipher_text , tag =  cipher.encrypt_and_digest(msg.encode("ascii"))

  return cipher_text , tag , nonce
```

In [4]:
```
def decrypt(cipher_text, tag, nonce):

  cipher = AES.new(key,AES.MODE_EAX,nonce=nonce)
  plain_text = cipher.decrypt(cipher_text)

  try:
    cipher.verify(tag)
    return plain_text.decode("ascii")
  except:
    return False
```

In [5]:
```
key = token_bytes(16) # 16 byte = 128 bit key
```

In [6]:
```
cipher_text, tag, nonce = encrypt(input("Enter plain text : "),key)

plain_text = decrypt(cipher_text, tag , nonce = nonce)
```

```
Enter plain text : Program of AES Algorithm
```

In [7]:
```
if(plain_text==False):
  print("Message has been corrupted")
else:
  print(f'\nPlaintext : {plain_text}')
  print(f'Key : {key}')
  print(f'Ciphertext : {cipher_text}')
```

```
Plaintext : Program of AES Algorithm
Key : b'C \n\x97R(:\xd5z\xbbg6=8\x84v'
Ciphertext : b'\xd1\xee\x04\x9e72\xef\xf4e\xb9\xb3\xbe7#/\x94\x08\xc1\xf0\x05
X$\x90\x9d'
```