Final Year B. Tech. (CSE) – I: 2022-23

4CS451: Cryptography and Network Security Lab

Assignment No. 7

PRN: 2019BTECS00077 **Batch: B7**

Full name: Biradar Avinash Vishnu

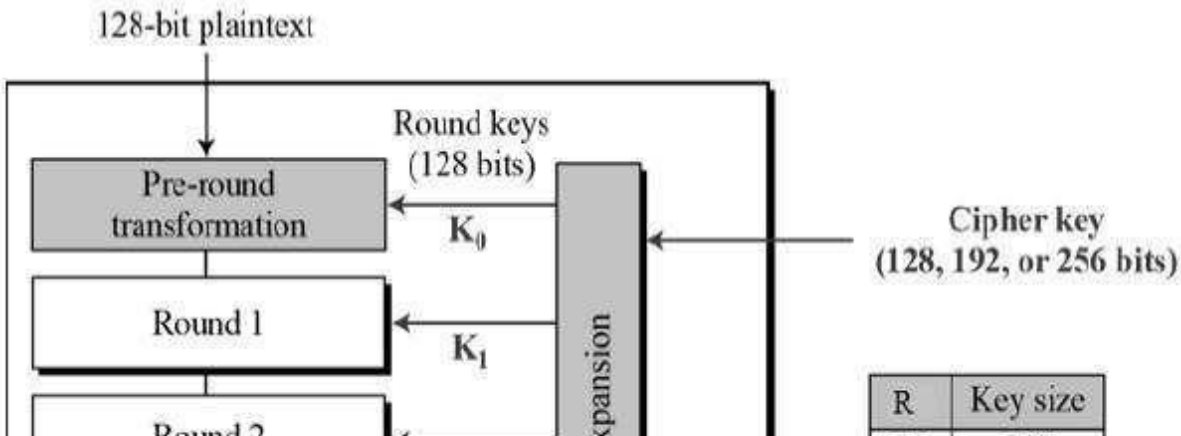
Title: Advanced Encryption Standard

Objective: To study and implement encryption and decryption using AES **Theory:**

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

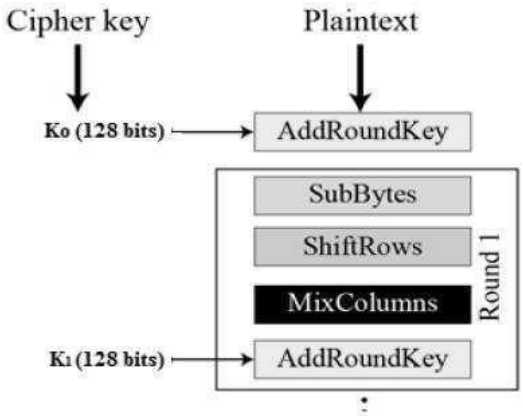
AES is a block cipher. The key size can be 128/192/256 bits. It encrypts data in blocks of 128 bits each. That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

The schematic of AES structure



Encryption:

A typical round of AES encryption comprises of four sub-processes. The first round process is depicted below –



Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

1. First row is not shifted.
2. Second row is shifted one (byte) position to the left.
3. Third row is shifted two positions to the left.
4. Fourth row is shifted three positions to the left.

The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes.

This step is not performed in the last round.

Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Code:

```python
import hashlib
from Crypto import Random
from Crypto.Cipher import AES
from base64 import b64encode, b64decode

class AESCipher(object):
    def __init__(self, key):
        self.block_size = AES.block_size
        self.key = hashlib.sha256(key.encode()).digest()

    def encrypt(self, plain_text):
        plain_text = self.__pad(plain_text)
        iv = Random.new().read(self.block_size)
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        encrypted_text = cipher.encrypt(plain_text.encode())
        return b64encode(iv + encrypted_text).decode("utf-8")

    def decrypt(self, encrypted_text):
        encrypted_text = b64decode(encrypted_text)
        iv = encrypted_text[:self.block_size]
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        plain_text = cipher.decrypt(encrypted_text[self.block_size:]).decode("utf-8")
        return self.__unpad(plain_text)
```

```python
    def __pad(self, plain_text):
        number_of_bytes_to_pad = self.block_size - len(plain_text) % self.block_size
        ascii_string = chr(number_of_bytes_to_pad)
        padding_str = number_of_bytes_to_pad * ascii_string
        padded_plain_text = plain_text + padding_str
        return padded_plain_text

    @staticmethod
    def __unpad(plain_text):
        last_character = plain_text[len(plain_text) - 1:]
        return plain_text[:-ord(last_character)]

key = input("Enter key:")
obj = AESCipher(key)
str = input("Enter input:")
cipher = obj.encrypt(str)
print(cipher)
plain_text = obj.decrypt(cipher)
print(plain_text)
```

Output:

```
D:\Study Material\Sem 7\CNSP>aes.py
Enter key:thats my kung fu
Enter input:attack at dawn
Encrypted text:  QuIDBwqtLtPnRWiZIHJbsDrUKe+aUSbr2jR4KT/7MhU=
Decrypted text:  attack at dawn
```

```
D:\Study Material\Sem 7\CNSP>aes.py
Enter key:occurrence
Enter input:send me more money
Encrypted text:  bGqzNduDjIc5f4Glc9Zx6YI65MwEzmzbxNJpqw9VjYZSrfgqhmHZR8zXoZvGZRo5
Decrypted text:  send me more money
```

File input

```
D:\Study Material\Sem 7\CNSP>aes_file.py
Enter key:gravity fall

Input file text: Studying is the main source of knowledge. Books are indeed never failing friends of man. For a mature m
ind, reading is the greatest source of pleasure and solace to distressed minds. The study of good books ennobles us and
broadens our outlook. Therefore, the habit of reading should be cultivated. A student should never confine himself to hi
s schoolbooks only.

Encrypted text:  m3fpUZ1mRkPJ8HJMHPMAUbM6Y7NxcKb##4sfVV8Mbd7/+Tbj6skPlIGlHuZaT+rciqoDmQWiTU4tPOXty5GT0HWoIF6sP75Xn73kLLpM
Y/rMdHq9DFUCHz7cKCtSa2zQ/a5Jqa5fqYaQWVJBFw2zx+2Qp4QZ1OIU7MCEG+q1kuoxPDmRz9u9kW0S10f8DKomLlRZOQaO2rzyhxXk7gK9KGqtEXEAjA55
6eaws+oldkfEiP07D/MqjruyNaxADjvbwIe5fCC+7301Ntpzrl/+SstQHIrxWZDErlEEq0BPrG8+GhZukCqmIrVqw5XDTu6Mxx9DcEiggoki+xoDmSps5gJB
5n7Y0lG9CfKTNdgzsQbNVOUAM7lOoRKQJslVP75N/HZz4tf+mXunEdRZvRwQEceCWygDpMPt+L66Dve3VJY0K8o5/sZD5Q0bbb4e815Bt7reId78drPMmTe9
mqGFLeIzpq+09GCNmyyCTjaxYq44Hsh1f73i+kKmQxE53LANI

Decrypted text:  Studying is the main source of knowledge. Books are indeed never failing friends of man. For a mature m
ind, reading is the greatest source of pleasure and solace to distressed minds. The study of good books ennobles us and
broadens our outlook. Therefore, the habit of reading should be cultivated. A student should never confine himself to hi
s schoolbooks only.
```