Assignment 2 - Project 1: AES

Aman Mehra (2017017) **Aditya Bhadoo(2017008)**

AES System -

Here we implement AES in python. Each segment of the Encryption - Decryption system, is implemented in the code. To test the system two 128 bit plaintexts represented in hexadecimal are encrypted and decrypted using a key **k**. The difference between the original and decrypted plaintext is shown to be zero, demonstrating their equality.

The system has three crucial parts - the encryption function, decrpytion function and the key management system.

The encryption function implements a 10 round AES encryption while the decryption contains the corresponding decryption code.

The key management system is implemented through a class (KeyManager). For a given 128 bit key, this pre-computes keys for each round of encryption and decryption and stores it in a buffer. An instance of this class is passed to the encryption and decryption functions to use for the ADD_ROUND_KEY step of the algorithm.

Verifying outputs -

We use two **plaintexts** to validate the correctness of the system. They are -
1. **0x1023456789abcdeffd325973ca2b310c**
2. **0xfd325973ca2b310c1023456789abcdef**

They **key** used to encrypt both plaintexts is the same and is -
0x770A8A65DA156D24EE2A093277530142

The below image depicts the output of the system for the two inputs.
The first row is the original plaintext. The second the corresponding ciphertext and the third the decrypted plaintext.
The last row shows the difference between the decrypted and original plaintext. As can be seen for both test inputs, this difference comes out to be **0** validating the efficacy of the system.

```
Original Plaintext =  0x1023456789abcdeffd325973ca2b310c
Ciphertext =  0x1b496c07ccbbf8474419ec904f74ef20
Decrypted Plaintext =  0x1023456789abcdeffd325973ca2b310c
Verification : Decrypted plaintext - Original plaintext =  0
```

```
Original Plaintext =  0xfd325973ca2b310c1023456789abcdef
Ciphertext =  0x5e52dde6f4d8bbcfab1100759a77e8ce
Decrypted Plaintext =  0xfd325973ca2b310c1023456789abcdef
Verification : Decrypted plaintext - Original plaintext =  0
```

Verifying intermediate states -

Below depicts the hexadecimal value of corresponding states in the encryption and decryption pipeline. The difference between each corresponding state is shown to be zero to validate their equivalence.

Output for plaintext - **0x1023456789abcdeffd325973ca2b310c**

```
Verifying Intermediate States of each round during encryption and decryption
Format - Encryption state , Decryption state , Difference (Should be 0)

0x6feb17fde463685511b1a3e064177fc6 0x6feb17fde463685511b1a3e064177fc6 0
0x8cd4ff21f191f1d56f8fd1bbe0378d75 0x8cd4ff21f191f1d56f8fd1bbe0378d75 0
```

Output for plaintext - **0xfd325973ca2b310c1023456789abcdef**

```
================================================================================
Verifying Intermediate States of each round during encryption and decryption
Format - Encryption state , Decryption state , Difference (Should be 0)

0x82fa0be9a7e394b6fca0bff427978325 0x82fa0be9a7e394b6fca0bff427978325 0
0x7bcc143ff937c5f5167c73302874e901 0x7bcc143ff937c5f5167c73302874e901 0
```