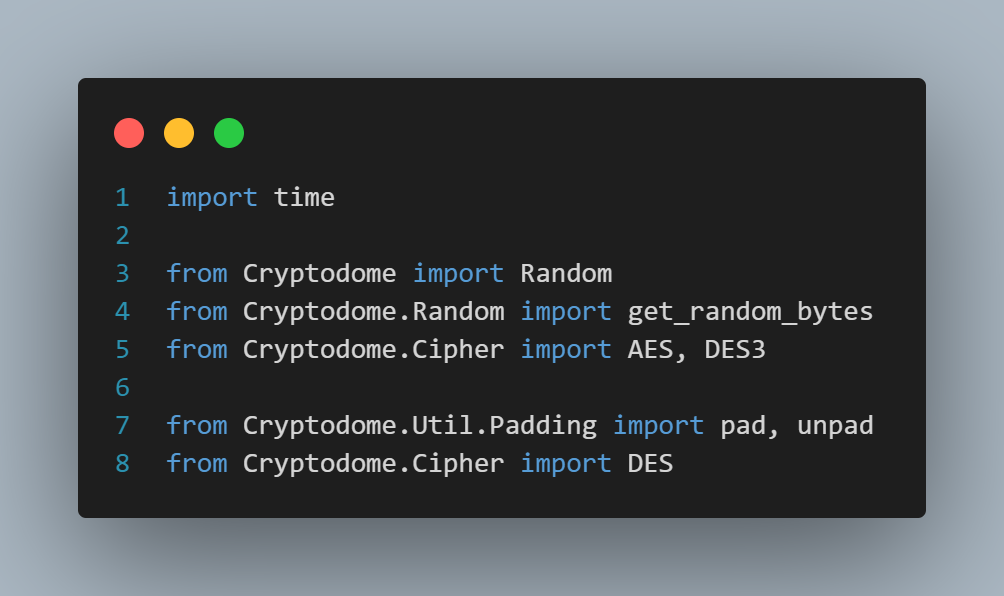
**Q. Measure and compare the time taken for encryption and decryption using DES, 3DES, and AES, with different input sizes. Analyze the three algorithms and identify which components made an algorithm particularly fast/slow, weak/strong. You can implement your own algorithms or use others’ implementation.**

**Before Starting** will import time and PyCryptodomex library to get started

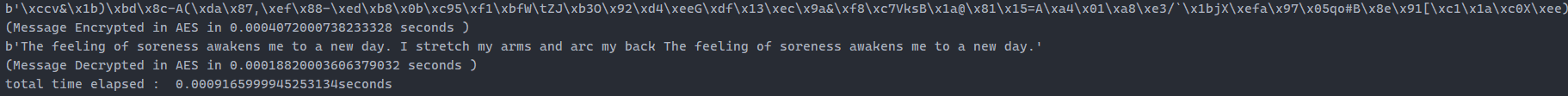


**1. AES:**

Advanced Encryption Standard (AES): AES is an acronym for Advanced Encryption Standard, a symmetric block cypher with a fixed data block size of 16 bytes. A 256-bit key can be used. I'm working with 16 bytes for my AES encryption algorithm

For Encryption, Firstly I’m generating a 16-bytes key randomly, and then I’m constructing an AES cipher in AES.MODE\_ECB Mode and passing it the key that was randomly generated in the first step, then I’m using my Cipher which I constructed before to encrypt our Message(Padded)

Secondly for decryption, I’m Constructing a decipher with AES.MODE\_ECB and passing it the key, and then I’m using my decipher to decrypt our AES encrypted message and then Unpadding our message to retrieve original message



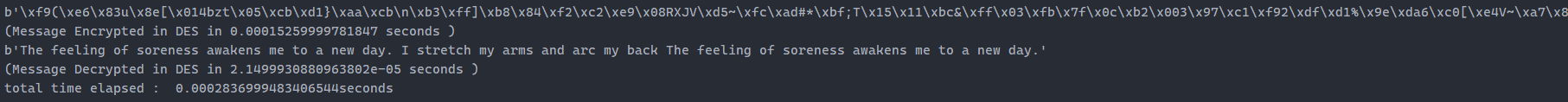
**Code:**

**2. 3DES:**

A fixed data block size of 16 bytes will be used for the symmetric block cypher **Triple DES**. It consists of three single DES cyphers cascaded together. The 16-byte key will be generated randomly. Here, we'll use a length of 16 bytes and a random number of bytes, and if it succeeds, we'll break; if not, we'll only do value error.

For Encryption, Firstly I’m generating a 16-bytes key randomly, and then I’m constructing an DES3 cipher in DES3.MODE\_ECB Mode and passing it the key that was randomly generated in the first step, then I’m using my Cipher which I constructed before to encrypt our Message(Padded)

Secondly for decryption, I’m Constructing a decipher with DES3.MODE\_ECB and passing it the key, and then I’m using my decipher to decrypt our DES3 encrypted message and then Unpadding our message to retrieve original message



**Code:**

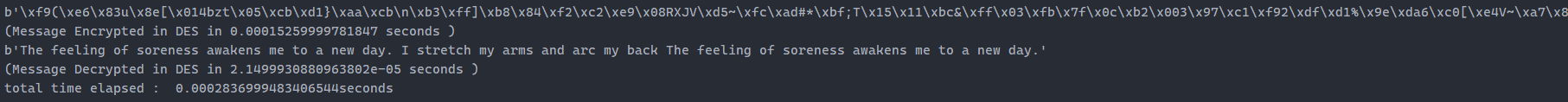


**3. DES:**

Data Encryption Standards (DES) is an acronym for a symmetric block cypher with a fixed data block size of just 8 bytes.

For Encryption, Firstly I’m generating a 8-bytes key randomly, and then I’m constructing an DES in DES.MODE\_ECB Mode and passing it the key that was randomly generated in the first step, then I’m using my Cipher which I constructed before to encrypt our Message(Padded)

Secondly for decryption, I’m Constructing a decipher with DES.MODE\_ECB and passing it the key, and then I’m using my decipher to decrypt our DES encrypted message and then Unpadding our message to retrieve original message



**Code:**

