2. **Attack on 2DES encryption (4 marks)**

Data Encryption Standard(DES) is a symmetric-key encryption scheme that was developed by IBM in the 1970s. Over the years, its susceptibility to numerous attacks, particularly brute-force attacks, has been revealed. Consider the following variant of the DES scheme used in our problem:

- $\mathsf{DES.Enc}(m, k)$*:* This is the encryption function. In our case, the key k is restricted to be of $n = 20$ bits. DES can only handle messages having length in multiples of 64 bits
- $\mathsf{DES.Dec}(\mathsf{ct}, k)$*:* This is the decryption function. The key k is restricted to be of $n = 20$ bits. The input ciphertext ct must have a length in multiple of 64 bits.

A variant of the DES scheme known as 2DES attempts to enhance security by applying 2 rounds of DES Encryption sequentially. In this problem, our attack will be on the 2DES scheme defined below:

- $\mathsf{2DES.Enc}(\mathsf{k} = (\mathsf{k}_1, \mathsf{k}_2), \mathsf{m}) = \mathsf{DES.Enc}(\mathsf{k}_2, \mathsf{DES.Enc}(\mathsf{k}_1, \mathsf{m}))$
- $\mathsf{2DES.Dec}(\mathsf{k} = (\mathsf{k}_1, \mathsf{k}_2), \mathsf{ct}) = \mathsf{DES.Dec}(\mathsf{k}_1, \mathsf{DES.Dec}(\mathsf{k}_2, \mathsf{ct}))$

Unfortunately, as discussed in class, the above 2DES scheme does not provide any extra security over the original DES protocol due to "meet in the middle" attack on 2DES. You are required to implement this attack.

Files Given: You are given the following python files on Teams COL759_A1_Coding2.zip:

- des.py:
  - It has three functions. The first one is key_gen(index) which takes an index and returns you the corresponding key. For example, if n (the number of bits of key) = 2 then there would be 4 keys so you can access these 4 keys by giving indices from 0 to 3.
  - Second function is encrypt(key, message) which takes key and a string message to return the encrypted message using a single DES.
  - Third function is decrypt(key, message) which takes key and a ciphertext to return the message corresponding to this ciphertext using decryption of single DES.
  - You can use these function to implement the attack.
- attack.py:
  - You are required to implement the attack(message, ciphertext) function in this file which takes a message and corresponding ciphertext generated using 2DES.
  - It is supposed to return the two keys which are used during the encryption (as a tuple). So for example, if the keys are key1, key2 (key1 is used first and then key2) then you have to output (key1, key2) and not (key2, key1) or anything else.

- You are allowed to make calls to encrypt(key, message) and decrypt(key, CT) functions of des.py.

Instructions:

- You would need to install the python3 and pycryptodome python packages to run the given files. Installation instructions can be found on this link
- You are only required to submit attack.py, with your implementation of attack(message, ciphertext). You don't need to submit any other files.
- Submit the attack.py file on Gradescope in the Assignment1 Coding2 assignment
- Your submission will be checked on multiple key pairs and on multiple messages. All test cases will be public.