Lab 01: Meet in the middle attack

**Introduction:**

In this lab, we implement a simple DES algorithm using python with encryption and decryption functions. After SDES is implemented, we develop a simple Double DES algorithm and prove the weakness of the algorithm using meet in the middle attack. We will compare the time taken to do the attack vs brute force attack on Double DES algorithm.

**Procedure:**

1. We will develop a simple DES algorithm using python. This algorithm has 8-bit plain text with a 10-bit key for encryption. Using the 10-bit key, we will generate 4 round keys which will be used in 4 rounds of encryption/decryption in SDES.
2. The SDES is used to develop Double DES algorithm which is using SDES twice to encrypt and decrypt given plaintext/ciphertext.
3. We will implement a meet in the middle attack which will try to find a key that will decrypt given plaintext/ciphertext pairs.
4. We will also implement brute force attack that will brute force to find keys that will decrypt given plaintext/ciphertext pairs.
5. Using the keys discovered, we will decrypt the given ciphertext in hexadecimal format.

**Results:**

A computer screen with white text

Description automatically generated

1. We found two keys k1 = 1101000101 and k2 = 1001110101 from the attacks we performed.
2. The time taken for Meet in the middle attack is 5.73 seconds where as brute force attack takes 20.60 seconds to find the same keys.
3. This shows how effective the meet in the middle attack is for finding keys for Double DES algorithm. Almost 3x time improvement over brute force attack.
4. We use these keys to decrypt the give ciphertext message in hexadecimal:

0xfb7cf0addb5a904590d4070be8fc9502c5506f85707e484e5457c39ccae19b66b0d36c7e03b2754cc36720d9cafa473c3fdff530d09aa20d19c5213f5c9727a3b7ecda681b0bc2bbaa754cf78921b84d1b64f0be150ac28e40816720f1be2aa0f31108fefcad6e332d3fdff5f4f4eab7

1. Since we have designed our algorithm to work on bits, we have to convert this message to bits and divide it into 8-bit blocks to make it work with Double DES algorithm we developed.
2. The decrypted message is :

**I am impressed that you were successful in decrypting this message. Do not tell anyone! Oh, and congratulations.**

1. We also discovered weak keys in our SDES algorithm using a simple python program.

**Number of weak keys found: 4**

**Weak keys:**

**0000000000**

**0001110101**

**1110001010**

**1111111111**