William Atkins

2/27/2022

CMSC 487

Project: "Meet in the Middle Attack Against DS-DES"

1) See code attached in blackboard

2) The two common simple 2DES keys between the plaintext/cipher pairs are
   Key 1: 831 ***or 0b1100111111*** ***or 0x33f***
   Key 2: 339 ***or 0b101010011*** ***or 0x153***

3) See code attached in blackboard

   Time for meet-in-middle was found to be around *0.27625 seconds*.

```
Finished!
The i keys were found to be [831]
The j keys were found to be [339]
Total time in seconds: 0.27625203132629395
```

4) See code attached in blackboard

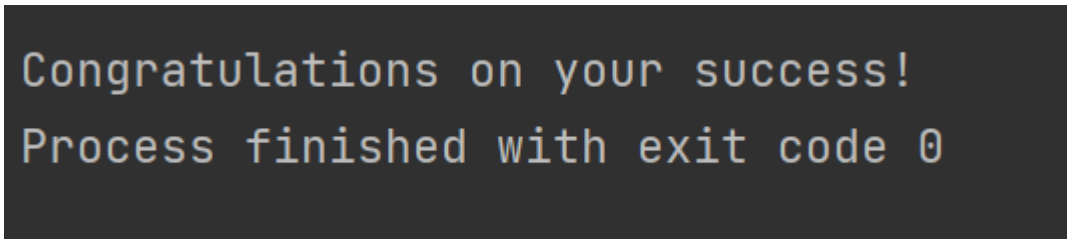
   Time for brute force of all keys was around *28 seconds*

```
The i keys were found to be [831]
The j keys were found to be [339]
Total time in seconds: 27.593255758285522
```

5) See code attached in blackboard

   Message:

Congratulations on your success!



6)

Weak Simple DES Keys:

This happens when permutation choice 1 results in 1's and 0's in the round/shift keys. As in when the first permutation splits the left and right into 1's and 0's. This will result in keys with all 1's, all 0's or the same pattern of 1's and 0's making the encryption very weak.

Key 1: 0b1111111111

Key 2: 0b0000000000

Key 3: 0b0111101000

Key 4: 0b1000010111

PC1: **3, 5, 2, 7, 4, 10, 1, 9, 8, 6**

1, 1, 1, 1, 1, 0, 0, 0, 0, 0

OR 0, 0, 0, 0, 0, 1, 1, 1, 1, 1