Assignment Content

For this project, you will be learning about DES from a simplified version and about the Meet in the Middle attack. You will implement the Simplified Data Encryption Standard (S-DES), a Feistel cipher based off DES with a block size of 8-bits and a key size of 10-bits. You may use the language of your choice, but it would be best to use one that supports bit manipulations. (It can be done in python3 for example, if you install and use the bitstring package. C of course, supports bit and byte operations, but not of arbitrary sizes.) To test your system, you may use the S-DES test vectors in the S-DES Known Answer Test document. Once you have completed your implementation, you will use it to mount a Meet in the Middle attack to determine the 20-bit key bundle (k1, k2) used in the Double S-DES encryption used in ECB mode to produce the following known plaintext/ciphertext pairs:

Plaintext/Ciphertext = 0x42/0x52, 0x72/0xf0, 0x75/0xbe, 0x74/0x69, 0x65/0x8a

Time the execution of your Meet in the Middle attack.

After finding the key with the Meet in the Middle attack, implement a brute force search for the key and time the execution of the brute force search.

After finding the key, use the key with the IV = 0x9c to decrypt the following text that was encrypted using DS-DES in Cipher Block Chaining mode with the key you found. The encrypted text is ASCII so convert the output to ASCII characters to read the message.

Ciphertext in hexidecimal = 0x586519b031aaee9a235247601fb37baefbcd54d8c3763f8523d2a1315ed8bdcc

What to turn in.

1. The commented code for your implementation of S-DES.

2. The key used to produce the ciphertext in the known plaintext/ciphertext pairs.

3. The code you used to implement your Meet in the Middle attack, along with the time your attack took to determine the key.

4. The code for your brute force key search, along with the time it takes to uncover the key.

5. The decryption of the text encrypted using CBC mode with the key you discovered and the code you used to decrypt it.

6. A list of the S-DES weak keys.

**Feedback for student**

**3/10/22, 1:03 PM**

**+28 Valid and commented code.**

**+2 Both keys correct.**

**+4 Valid MITM code.**

**+1 MITM time.**

**+0 Invalid Brute force code. Performs MITM again.**

**+1 Brute force time.**

**+4 Valid CBC code.**

**+2 Correctly decrypted text.**

**+4 Correctly identified weak keys**