Assignment

Programming project: Simplified DES, meet-in-the-middle attack

30 points

Using the encryption and decryption methods you wrote for SDES, write a program called **`SDESMitm.java`** or **`sdesmitm.py`** that will carry out a meet-in-the-middle attack on 2SDES. This system encrypts a plaintext first with one key and then again with a different key. Please review the attack in the notes and the textbook. Recall that this is a known-plaintext attack. I will provide plaintext/ciphertext pairs. Based on those, you should be able to recover the two 9-bit keys.

Write the program so that it can be run from the command line taking four parameters:

1. plaintext 1 integer
2. ciphertext 1 integer
3. plaintext 2 integer
4. ciphertext 2 integer

Two pairs are needed because the first plaintext/ciphertext pair will let you create a shorter list of key pairs and the second plaintext/ciphertext pair will allow you to narrow that list down to one key pair. When run, the program should print the two keys.

Submission instructions

Please make sure your name appears in comments at the top of the source file and that the program file is given the name I specifed above. Not doing either of these will cost points. Submit the .java or .py file (not zipped!) to the D2L submission folder provided for it.

Document last updated on February 14th, 2021.