CSE 825 Fall 2020
Assignment 1

In this assignment, you are to implement the DES encryption algorithm as well as breaking it. You will follow the details of the algorithm (i.e., table, *S*-box, etc) using the following link:

`http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm`

Here's the detailed instructions:

1. This is a group assignment.
2. Use your favourite programming language for implementation of the algorithm.
3. Recall that DES is a symmetric-key algorithm and the same algorithm is used for encryption and decryption. Make sure, your implementation works both ways.
4. You will share a ciphertext with another group (see the mapping table below). Let us call your group "*Group 1*" and the receiving group "*Group 2*". Group 2 is supposed to break the ciphertext using a brute force algorithm that enumerates all possible keys. This algorithm should break the ciphertext in less than one hour. Thus, it is the responsibility of Group 1 to provide Group 2 with the information on how to reduce the number possibilities of the 64-bit encryption key.
5. The original plaintext will be in English. Obviously manual observation and verification of the brute force algorithm is not practical. You are allowed to use any third-party code to automatically check whether an attempt to break the code results in meaningful English text.
6. Remember to apply padding when necessary.
7. There is no need for chaining.
8. Feel free to use parallel processing or any other technique to speed up cipher breaking. The group with the fastest algorithm will be recognized., given the same hardware platform.

Deliverable
Your are to provide Group 2 with your ciphertext and information on how to limit their search by **11:59pm on Monday, October 5** by email (CC me so I can keep track). Group 2 should report successful breaking of the code by Wednesday October 7, 11:59pm.

Group mapping: In the following mapping the inverse of Group 2 is Group 1 and vice versa!

Group 1	**Group 2**
drew-tyler-francisco	gabe-julia-shashank-greg
logan-nicole-reuben	mohamed-jacob
norah-arya-jesus	tzu-han-ritam-oyendrila
yuguang-yuanda-yiwen	gabe-julia-shashank-greg

Notice that gabe-julia-shashank-greg appears twice. That means they will have to work with 2 groups since they are a larger group.