Network Security Assignment #4
Meet-In-The-Middle Attack

Learning Objective

The goal of this homework is to understand how MITM attack works. The following five plaintext messages were encrypted by double Mini-AES (S-AES) using two different keys. Given their corresponding ciphertext messages, please utilize the MITM attack technique to figure out the key pairs used for the encryption.

1	**Plaintext**: Network Security class is awesome! **Ciphertext (binary)**: 00100100011100101001010001011000110001100000001001100101000001010000000001100010110011111011000110101111011100011010010001010001010100001011011010111110000010101101111101101110110000001011010000001011010101100111101011000011000001011000100011110110100111111011101001001010
2	**Plaintext**: Oh yeah! I Love NCKU, IIM~ **Ciphertext (binary)**: 11110110100111010110010111000100101111100010101010110111100110100110011111000100110101111100000111010110000011000110101001000101011110001011011000100001101100100101101110011110110111000001001000001111010100110000111010110000011000110101001000101011110001011011000100001101100100101101110011110110111000001001000001111010100111
3	**Plaintext**: Initial Impressions of the HTC 168 **Ciphertext (binary):** 00000111110100111100111011010111101101111110110100110101110010101010001111101001010110101110011000000010110001000101000000110000110100110100101010000101101010110110101101001110000110101110011011100001111010001100001111100111001010010000001011001001101110010011101011000
4	**Plaintext**: Mini-AES: A simplified variant of the Advanced Encryption Standard **Ciphertext (binary):** 11011100110000101001010001111001100100001000001001110011100001100001001011100011111000111111100110100000011000010110111101010101100111100000100110010111100010011100111000100111001101011100110011001010110000101011011111011010110010000000011100100000101101110110100111100101100011100001101001101010010001011101001010000101110101111000101100000100011110001100111000100111000001111100110100000100011110001010100000100001000101011100000100010111110101010110010010000101101111111011110110100010100001011011111010101100100100001011011111110111011010001010000101101111010101011001001000010110111111101111011010001010000101101111101010101100100100001011011111110111101101000101000010110111101010101100100100001011011111110111101101000101000010110111100000100010111110101010110010010000101101111111011110110100010100001011011111010101011001001000010110111111101111011010001010000101101111100000110100001111101110001

5	**Plaintext:** Chien-Ming Wang KC **Ciphertext (binary):** 1111000001101101110001111101000111110100100011111101110011000010011101000111001101100100001100111010001010000101011001111110010101111111111110110

Please read the following webpage on how-to use Mini-AES and converting text to/from binary strings in SAGE:

1. Mini-AES Reference Page
2. Utility Functions for Cryptography

Other detailed instructions:

1. Place the files in a folder called Rxxxx_hw4, where Rxxxx is your student ID
2. Zip the folder and upload the archive to our AACSB class page no later than **Nov. 22nd**