Homework Number: hw01

Name: Shu Hwai Teoh

ECN Login: teoh0

Due Date: Thursday 1/23/2020 at 4:29PM

1. Recovered plaintext quote:
2. Encryption key
   1. Binary: 1111111111111111
   2. Decimal: 65535
3. Explanation

To recover both the original quote and the encryption key, I did the following steps:

* 1. Reduce the PassPhrase ("Hopes and dreams of a million years") to a bit array of size BLOCKSIZE (16) as the first “previous\_decrypted\_block” for decryption.
  2. Create a bitVector from the ciphertext hex string in ciphertextFile (encrypted.txt).
  3. Carry out differential XORing of bit blocks and decryption for all possible keys to find the key.

1. Code