Homework Number: hw01

Name: Shu Hwai Teoh

ECN Login: teoh0

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

1. Recovered plaintext quote:

It is my belief that nearly any invented quotation, played with confidence, stands a good chance to deceive.

- Mark Twain

1. Encryption key
   1. Binary: 0110 0010 0111 0010
   2. Decimal: 25202
2. 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 (on the second page)

