HW01: Brute Force Attack

Homework Number: 01
Name: Jack Gardner
ECN Login: gardne97
Due Date: 1/19/23

Recovered plaintext quote: “Sir Lewis Carl Davidson Hamilton (born 7 January 1985) is a British racing driver currently competing in Formula One, driving for Mercedes-AMG Petronas Formula One Team. In Formula One, Hamilton has won a joint-record seven World Drivers' Championship titles (tied with Michael Schumacher), and holds the records for the most wins (103), pole positions (103), and podium finishes (191), among many others. Statistically considered as the most successful driver in Formula One history.”
Recovered encryption key: 4040
Brief explanation of code: cryptBreak.py contains a function called cryptBreak and a “__main__” section used to apply cryptBreak to the ciphertextfor all possible keys in the 0 to 2^16 key range. The key bit vector and ciphertext file are inputted into the cryptBreak function which returns the decrypted output text. Since the encryption and decryption algorithms are made public, the cryptBreak function is very similar to the DecryptForFun function provided to us; most notably, the BLOCKSIZE has been changed to 16 bits. When the decrypted text contains “Sir Lewis,” the loop breaks and the key and decrypted message are printed.