Recovered plaintext code:

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:

The cryptBreak.py contains the Python function def cryptBreak(), which takes in the name of the cipher text file as a string, and the key as a BitVector. This function essentially tries to recover the original quote and the encrypted key by executing a brute-force attack. The effective key size for this problem is 16 bits, so the keyspace has a size of 2^16. However, we are given that the string contains Sir Lewis, so the search space has been reduced. First, the program reduces to passphrase to a bit array of 16 bits. Then, the program creates a BitVector from the hex string read from the cipher text file. We also create another BitVector for storing the decrypted plaintext bit array. This program also uses differential XORing, which means that when a file is scanned in blocks of bits, the output produced will be made into a function of output for the previous block of bits. This means that the current output block depends on the previous output block. The reason for differential XORing is to reduce the chances of using repetitive patterns when encrypting messages and breaking the encryption by statistical analysis.