Assignment-2
Submission Deadline: 12 February, 2024

In this problem, you will play the role of a cryptanalyst and attempt to break a cryptographic system composed of the two Python scripts EncryptForFun.py and DecryptForFun.py discussed in the provided material. The script EncryptForFun.py can be used for encrypting a message file while the script DecryptForFun.py recovers that message from the ciphertext produced with the previous script.

Problem

With the parameter BLOCKSIZE set to 16, the script EncryptForFun.py produces the following ciphertext for a plaintext message that is a quote from Douglas Adams:

3c2b223a71277173636930742f6c296b33702e2a7d127b086b146c09721821083d092c112
645265e7b202574126f147c0b690b3d392d2b342b40

all in one line. You can assume that the passphrase stays the same (that is, the passphrase is "Hopes and dreams of a million years").

Your job is to recover both the original quote and the encryption key by mounting a brute-force attack on the encryption/decryption algorithms.

HINT 1: The correctly decrypted message should contain the words *Douglas Adams*.

HINT 2: The logic used in the scripts assumes that the effective key size is 16 bits when the BLOCKSIZE variable is set to 16. So your brute-force attack needs to search through a keyspace of size 2^{16}.

The program must be implemented and saved in a file named cryptBreak.py. This function must be implemented to decrypt the message *for a single key* and not to perform complete brute force analysis. The brute force analysis must be done within the code's main function/statement or in a

separate Python file by importing cryptBreak.py into that file. Note that the string returned by the above function may or not may not be the correct plaintext since the correct key bv is unknown. Therefore to determine the correct value for key bv, you will need to brute force all possible values for key bv and check the returned string to find the right one.