CM3110 Security Coursework Report

Part B:

My attack takes the bytes k1 to k2, which just happen to be “100GBP”. The program XORs the original cipher text 6 bytes which are ('9B', '88', '79', 'E7', '57', '27') with the plaintext “100GBP”. The result from this, I then XOR with “999EUR” (once I have converted this string to integers). I then output this result to Hexadecimal, which becomes the replaced k1 to k2, which I then overwrite in a new ciphertext file.

I need to know the exact values of the original plaintext, so I know which bytes I need to XOR, to make the replacement message eligible. If I XORd bytes at random, then I would not produce anything meaningful, and perhaps see ‘?’ in my new decryption as the values are not compatible.

NB: unfortunately, I had a user-created bug in part B, (see ln. 22), and struggled to fix it until I realise the problem at the very end of the deadline!

However, I have left the remaining code intact to show my logic.