**Cyber Security Assessed Exercise**

**Mary McDowall – 1003254m**

**Known Plain Text**

Key: 0x058C

Message: All I ask is a chance to prove that money can’t make me happy

**Ciphertext Only**

Key: 0x4DD0

Message: It is dangerous to be right in matters on which the established authority are wrong.

With a key space of size 65536 = 216 , the entropy of the key space is 16.

The natural redundancy of English is 3.2 so the unicity distance is 16/3.2 = 5.

Which means that it should be possible to find the key unambiguously with 3 blocks if we take it that each block contains 2 characters.

In actuality 11 blocks had to be decrypted in order to find the correct key.

**Time Memory Tradeoff**

Key: 0x9614

Message: I have not failed. I’ve just found 10,000 ways that won’t work