Assessed Exercise 1

Anders Kofoed - 2120935
2120935k@student.gla.ac.uk
Cyber Security - University of Glasgow

February 24, 2014

1 Known Plain Text Attack

Key found: 36460
[1] Decrypted message: An expert is a person who avoids the small errors while sweeping on to the grand fallacy

2 Cipher Text Only Attack

Key found: 21346
Decrypted message: His manuscript was both good and original, but the part that was good was not original, and the part that was original was not good

To determine the required number of blocks to decrypt the message, we can look at the unicity distance [1]. Since we have a key length of 16 bits, and we assume that all keys are equally likely or random, we get an key entropy of H(K=16) = 16. The redundancy of the English language is measured to be approximately D=3.2 [1]. This gives us an unicity distance of U= 16/3.2 = 5. Which means that in theory it should be sufficient with 5 blocks of data.
Number of blocks needed from experiment: 14
These results make sense, since my implementation used the pretty ineffective algorithm of looking for whole English, 3-letter words, a faster way would be to look for n-grams of length 2 or 3 [2]. I chose not to change

[1] Used code from provided classes; DecryptAllBlocks.-, Hex16.- and BlockToText.java as well as standard java.util and java.ui libraries.

my implementation since the assignment didn't present any requirements on performance.

3 Time Memory Tradeoff

Key found: 6232
[2] Decrypted message: Do not meddle in the affairs of wizards for they are easily angered

References

[1] Unicity Distance *Practical cryptegraphy* `practicalcryptography.com/cryptanalysis/text-characterisation/statistics/`

[2] Frequency analysis *Read 12:13PM, 24. February.* `http://en.wikipedia.org/wiki/Frequency_analysis`

[2] Used provided classes Table.-, DecryptAllBlock.-, Hex16.- and BlockToText.java as well as standard java.util and java.ui libraries.