

Assessed Coursework 1

SYMMETRIC ENCRYPTION

Jacob Cooper |H00251723 |Computer Network Security | 21/10/19

# Introduction

This is the first coursework for Computer Network Security (F20CN) on Symmetric Encryption. All work presented here is my own and any that isn’t has been given proper accreditation. Throughout this coursework I hope to understand the various methods used in Symmetric Encryption and how they are implemented so that I can have a greater understanding of how they work. Specifically I’m hoping it will deepen my understanding of the more complicated encryptions such as AES – 128 cipher and its modes of operation as well selecting a safe and robust IV for said encryptions. For task one I hope to understand the use of frequency analysis and how it shows Monoalphabetic Substitution Ciphers to be extremely vulnerable. For task 2 I hope to understand the application of a multitude of different ciphers and how effective they are. Task 3 seems to be the most complicated as such I’m hoping to learn a lot from it: I hope gain a further understanding of how AES-128 cipher and all its modes work as well as how they differ and which are more safe; I also hope to learn how a single-bit error affects the decryption of these encryptions; I would also like to learn about implementation of IV. For task four I would like to continue this learning about IV’s and how they play an important part in encryption integrity and how an attacker can exploit a poorly chosen IV. For task 5 I hope to understand how a brute force known-plain-text attack can be carried out (provided that a certain level of information is fulfilled) as well as how effective this strategy is.

# Task 1

### Conventions

One convention I did use was representing the cipher text with lowercase and the plain-text with upper case. This is to make it clear when deciphering which letters have been substituted in and are a part of the deciphered plain text and which haven't been substituted in and are a part of the original cipher text.

### Frequency analysis

Using the first resource resource provided (\*insert link here) I inputted the cipher text I was given into the resource and it provided me with the frequency of each of of the characters in the cipher

Using the second resource (\*insert link here) its clear that ‘e’ is the most frequent letter in most English plain-text and ‘h’ is the most frequent letter in the cipher text so I hypothesize that ‘h’ is actually ‘e’. This is backed up by ‘the’ being a common trigram in English plain-text and ‘bph’ being the most common trigram in the cipher text. So we can say that b=T , p = H and h=E .

### Substitution

To substitute the predicted letters into the cipher text I used the command

bash-4.2$ tr bpe THE

which is the command I will be using every time I substitute letters into the cipher. When ‘T’ ,‘H’ and ‘E’ were subbed in for ‘b’ , ‘p’ and ‘h’ there was no apparent problems and it opened up more possible exploration.

### Completing the words

From this start we got from frequency analysis we can continue on to decode the whole text we do this by completing words such as ‘THjEE’ that appear and substituting the obvious missing letter (in this case ‘j’ must be ‘R’ ) into the cipher text. I then repeated this process until I had the full decrypted plain text ( See Appendix 1).

# Task 2

# Task 3

# Task 4

# Task 5

# Summary