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 cyphers 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 attack can be carried out provided that a certain level of information is fulfilled as well as how effective this strategy is.