STUDY AND COMPARE THE STRENGTH OF CRYPTANALYSIS ALGORITHMS THAT ARE USED TO DECIPHER ENCRYPTED FILES

Prepared by: Ooi Ken Lee

ABSTRACT

This project study various techniques used to analyze the encrypted text. It aims to test the strength of the currently available encryption methods especially those commonly used for password protection on certain files. Some of the cryptanalytic techniques that are commonly used include ciphertext-only attack, known-plaintext attack, chosen-plaintext attack, main-in-the-middle attack and timing attack. Literature review will be done to compare the different techniques. I will study on how each cryptographic attack and cryptanalysis techniques work. The project will provide the results of the comparisons being done on the various techniques as well as point out the strengths and weaknesses of each technique that is being studies. Ultimately, this project will give those people who contemplate to design a new encryption algorithm a much deeper understanding of these cryptographic issues. The system that is designed will be an enhanced cryptanalysis technique that is able to decipher encrypted text.