

A STUDY ON CRYPTANALYSIS ALGORITHM

Prepared by: Gharry Bin Ghaffar

ABSTRACT

The Cryptanalysis Algorithm is used to break encrypted information. There are two categories of cryptographic algorithms: conventional and public key. This project study the various techniques used to analyze the encrypted text. The target is to test the strength of the current available encryption method especially those commonly used password protection on certain office suite. The encrypted data will be tested under several different techniques of decrypting methods in order to break the encryption itself. The program languages that will be used are to break the encryption itself. The program languages that will be used are C, C++, VB, Delphi and Perl which will be chosen from the various cryptanalysis programs that had been tested.