Practical – 13

Objective- Study of Cryptool to perform various encryption-decryption techniques

The CrypTool

Development of the CrypTool began in 1998 by various German Universities andcompanies, since then, it has become an open source project and has involved developers all over the world. Its purpose is to aid users with understanding the various concepts and techniques used in cryptography. The program covers a range of modern ciphers such as RSA, DES and AES as well as classically used cipher s including the Caesar, Playfair and Vigenère ciphers. CrypTool provides the user with a variety of tools designed to aid with analysis of messages. Such tools include Entropy, Floating Frequency, Histogram, N-Gram, Autocorrelation and Periodicity.

Areas of use

The CrypTool, boasting 3000 unique downloads a month, has arguably become the de facto tool for studying cryptography. It has two primary target markets:

Industry

Although it is not known exactly who uses the CrypTool (besides the download records and the explicit feedback given) it is thought members of the technology industry would be prime users. Fields where a user is extremely likely to use the software include military, government, banking, telecommunications and software development.

Universities

Primarily students and lectures of computing type courses are likely to use the software.

CrypTool Manual

This next section will be a selective breakdown of the tools and functions within the CrypTool and will give an explanation as to how to use each. This should be used as a reference when undergoing the lab sessions. For simplicity, this section will look at each of the menu headings in turn. It is worth noting at this point that the CrypTool contains an extensive online help file, which is very informative. Should you feel unsure at any point as to how to use a particular aspect of the application, press F1 and the relevant help page should be located.

File, Edit, View

Like the majority of Windows applications the menu buttons File, Edit and View have standard functionality allowing the user to save files, open them, edit them and alter the view of the program etc.

Encrypt/Decrypt

This menu button encompasses the cipher algorithms available with the CrypTool. They are broken down into four sections; Classic Symmetric, Modern Symmetric, Asymmetric and Hybrid. With a text file open, the user is able to encrypt or de crypt the data from this section.

Installation

To install CrypTool on any Windows type Operating System, simply download the version 1.4.10 from the website http://www.cryptool.org/ and double click on the executable SetupCrypTool_1_4_10_en.exe then follow the onscreen inst ructions.

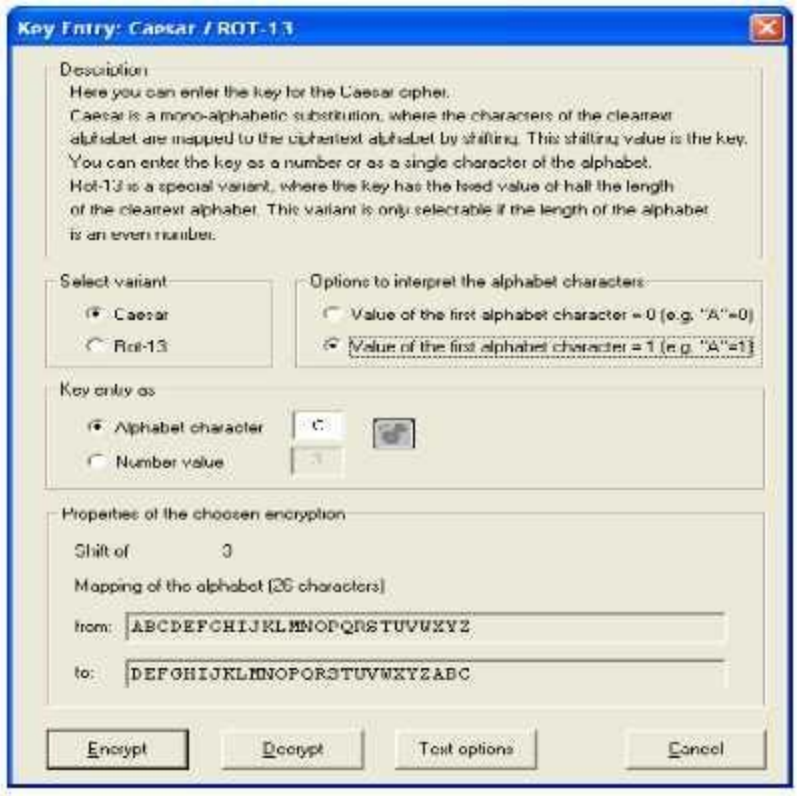
After installation, the file all you will need to use is CrypTool.exe.

The Caesar cipher

One of the more simple ciphers you can implement using the CrypTool is the Caesar cipher, this is a form of the substitution cipher and is explained in greater detail in the Report.

To begin with, open the CrypTool and go File > New. In the newly opened window type the message you wish to encode. The contents of your message is your personal choice, however, you should ensure its length is greater than 64 cha racters for the purpose of later analysis, in general the greater the length of your message the more accurate the later analysis will be. Alternatively, select the example text accompanying the CrypTool by clicking File > Open… and then selecting examples\Startingexample-en.txt.

Next select Crypt/Decrypt > Symmetric (classic) > Caesar / ROT-13… From here you will be presented with the option of encrypting with either Caesar or ROT-13 variants.



The key that you input here is the amount that the alphabet will be shifted by. You can enter the key as a letter of the alphabet or as a number. The letter will correspond to the shift of the alphabet, so for example A will shift the alphabet by 1 or 0, as it is the first letter in the alphabet, B by 2 or 1 as it is the second etc. ROT-13 is an abbreviation for Rotate by 13 places, and so would have a key of M (if the 1 alphabet character is assigned the value 1) . Additionally, the shifted alphabet is demonstrated below to clearly illustrate what the cipher wil l do.

Once you have selected your key select Encrypt. A new window will open with your encrypted message. Now you can analyse the strength of the encryption using a variety of techniques.