1. Lab Cryptool No. 1

1. Download and install Cryptool. http://www.cryptool.org/ .
2. Encrypt and decrypt a message with a symmetric encryption algorithm for example DES, AES, IDEA, 3DES etc.
3. Encrypt a text message with a symmetric encryption algorithm, and e-mail it to one of the other students in this course. Supply him with the necessary information, so he can decrypt it.
4. Encrypt a message with DES and decrypt it with triple DES, and opposite encrypt a message with triple DES and decrypt it with DES.
5. Use Cryptool to make a brute force attack on DES. How long time will it take for your computer to compromise a secret key.
6. A DES encrypted message is placed in Exercise folder on Fronter the filename is DES. You have been lucky, you have seen some part of the key 12 34 56 78 90 ?? ?? ??. How long time will it take you to compromise the complete key by using a brute force attack?
7. Many classic encryption algorithms exist. One of them is the Caesar algorithm. Read about the Caesar encryption algorithm in "Cryptool – help". Try to encrypt and to decrypt text messages with the Caesar algorithm.
8. The following message is encrypted with the Ceasar algorithm. Try to decrypt it - first manually and second automatically with some of the tools from Cryptool.

MbizDyyv

Drsc sc k dohd psvo, crygx sx ybnob dy rovz iye dy wkuo iyeb psbcd cdozc gsdr MbizDyyv.

1) Yxo drsxq iye mkx ny o.q. sc dy oxmbizd drsc psvo gsdr dro Mkockb

kvqybsdrw (fsk dro woxe "Mbizd \ Mvkccsmkv").

2) Dro locd yfobfsog klyed kvv pokdeboc yp MbizDyyv sc yppobon li

dro cdkbdsxq zkqo yp dro Gsxnygc yxvsxo rovz grsmr myxdksxc vsxuc dy kvv bovofkxd pexmdsyxc.

Iye mkx mkvv ez dro cdkbdsxq zkqo fsk dro woxe "Rovz \ Cdkbdsxq zkqo" yb ecsxq dro cokbmr uoigybn

"Cdkbdsxq zkqo" gsdrsx dro sxnoh yp dro yxvsxo rovz.

3) Oczomskvvi dro ohkwzvoc (dedybskvc) zbyfsnon gsdrsx dro yxvsxo rovz wkuo sd okci pyb iye dy qod

ez dy czoon. Droco zkqoc mkx lo pyexn fsk dro woxe "Rovz \ Cmoxkbsyc".