CPTR 427 Lab #02 Name

Symmetric Encryption Tools

# Introduction

The purpose of this lab is to introduce you to symmetric encryption algorithms and their uses and weaknesses. You will need a partner for this lab. In addition to classic encryption (e.g. substitution ciphers such as the Vigenère cipher) we consider 3DES, AES and BlowFish.

# Lab Goals

1. Decrypt a recently discovered Vigenère cipher, and determine why it is not safe to use classic encryption algorithms.
2. Encrypt and Decrypt using AES, 3DES and BlowFish.
3. Research password security applications.

## Setup:

1. You need internet access!
2. You will need a windows machine (you may use your virtual machine if you like)

## Lab Operations

1. Read the story at: <http://www.foxnews.com/us/2010/12/25/civil-war-message-opened-decoded-help-coming/> and decipher the message. Hint: The key is two words and a total of 15 letters long. Since the words are separated for you, single letter letter words may be extremely useful in your decryption. For your convenience, the encrypted message is given below:

SEAN WIEUIIUZH DTG CNP LBHXGK OZ BJQB FEQT XZBW JJOY
TK FHR TPZWK PVU RYSQ VOUPZXGG OEPH CK UASFKIPW PLVO
JIZ HMN NVAEUD XYF DURJ BOVPA SF MLV FYYRDE LVPL
MFYSIN XY FQEO NPK M OBPC FYXJFHOHT AS ETOV B OCAJDSVQU
M ZTZV TPHY DAU FQTI UTTJ J DOGOAIA FLWHTXTI QLTR
SEA LVLFLXFO
2. Download and install ABI-CODER. Encrypt and use it to exchange a question and answer with your partner.
	1. Each partner should encode a question and send it to their partner via email.
	2. Each partner should encode an answer and reply to their partners question.
	3. Show me the original file, the sent email, the response email and the decrypted answer.
	4. Repeat this for each type of encryption and answer the questions in section 1 below
3. Research: What password managers are available today? List the top 3 popular ones and reference sites that helped you determined which ones were popular. What algorithms do each of these use?

|  |  |
| --- | --- |
| Top three Apps in order | Algorithm(s) used |
|  |  |
|  |  |
|  |  |