Applied Cryptography

**Lab 6 - Symmetric Key Cryptography**

# lab: Deciphering Secret messages

In this lab you will decipher messages that are encrypted using the classical shift cipher. You are encouraged to do decrypt by hand first and resort to the tool available at the link provided below or other tools you find on the Internet to automate the process.

You can use the tools at the links below or other resources you find for frequency analysis.

<http://practicalcryptography.com/cryptanalysis/text-characterisation/monogram-bigram-and-trigram-frequency-counts/>

<http://www.simonsingh.net/The_Black_Chamber/substitutioncrackingtool.html>

Answer these questions:

1. Which method would you suggest be used to break this cipher? Brute force or frequency analysis? Why?
2. Use the method you suggested in part a. to break the cipher. Provide explanations for each step.
3. What is the plaintext?
4. What is the key that was used to encrypt the message?

### A Shift Cipher: What does the text say?

fxxmjbfxltnslymwtzlmymjbttixxmjrjybnymfbtqkbmtmfifajwdlwjfyrnsiytjfymjwzugzymjifwjistygjhfzxjtkxtrjbttihzyyjwxbtwpnslsjfwgdnsymjktwjxymjfxpjimjwbmjwjxmjbfxltnslymjuttwhmnqibmtinistypstbymfynybfxifsljwtzxytxyfdfsiyfqpytfbtqkxfniytmnrnfrltnslytxjjrdlwfsirtymjwfsi hfwwdmjwfhfpjfsifqnyyqjutytkgzyyjwkwtrrdrtymjw

### Fun challenge: A Substitution Cipher: What does the text say?

zorxv dzh yvtrmmrmt gl tvg evib grivw lu hrggrmt yb svi hrhgvi lm gsv yzmp zmw lu szermt mlgsrmt gl wl lmxv li gdrxv hsv szw kvvkvw rmgl gsv yllp svi hrhgvi dzh ivzwrmt yfg rg szw ml krxgfivh li xlmevihzgrlmh rm rg zmw dszg rh gsv fhv lu z yllp gslftsg zorxv drgslfg krxgfivh li xlmevihzgrlm hl hsv dzh xlmhrwvirmt rm svi ldm nrmw zh dvoo zh hsv xlfow uli gsv slg wzb nzwv svi uvvo evib hovvkb zmw hgfkrw dsvgsvi gsv kovzhfiv lu nzprmt z wzrhb xszrm dlfow yv dligs gsv gilfyov lu tvggrmt fk zmw krxprmt gsv wzrhrvh dsvm hfwwvmob z dsrgv Izyyrg drgs krmp vbvh izm xolhv yb svi

## Grading Rubric

|  |  |
| --- | --- |
|  | Max. Points |
| Deciphering shift cipher | 50 |
| Answers to 4 questions | 50 |
| Total | 100 |