Introduction to Computer Security – G6077

Lab 5b Sheet

This sheet covers:

* Understand and perform matrix calculation
* Understand frequency analysis
* Practice different ciphers by completing online challenges
* Use online tools like CrypTool

# Matrix calculation (Matrices plural)

Matrix is one of the concepts that is used in many different ciphers. It is a way to represent information in the form of rows and columns. If you do not know about matrix, please read on the matrix following two links.

Source 1: <https://www.mathsisfun.com/algebra/matrix-multiplying.html>

Source 2: <https://www.khanacademy.org/math/precalculus/precalc-matrices>

Complete these questions

|  |  |  |
| --- | --- | --- |
| **Question** | **Matrices** | **Answer** |
| Write dimensions for these matrices. |  |  |
|  |  |
|  |  |
|  |  |
| Find the product of each pair of the matrices |  |  |
|  |  |
| Find the inverse of each of the matrix, if it exists. |  |  |
|  |  |
|  |  |

You must not use online calculator to solve the above questions. You should use it only to check your answers.

# Frequency analysis

Frequency analysis is one of the key concepts used in cryptanalysis. It is used to dig deep in the cipher text to perform analysis on single character, digrams and trigrams etc. It is used in many other ways to find information about the plaintext from the cipher text. If you do not know the basic, you should follow the link below to find out about frequency analysis.

<https://www.mathsisfun.com/data/frequency-distribution.html>

# Practicing ciphers / Cipher challenges

In lecture we have covered the following ciphers

* Caesar
* Rot-n
* Affine
* X-OR
* Playfair
* Hill cipher
* Vigenere
* Vernam
* Rail fence
* Route / Rectangular

Click on the [link](https://asecuritysite.com/challenges) to access an external resource. The external resource has examples and a number of tasks to complete on each cipher. You should complete tasks of those ciphers that we have covered in our course so far. You should be using pen and paper to complete the tasks. You will need to compare it against answers by your friends to double-check it.

<https://asecuritysite.com/challenges>

# CrypTool – Online tool

CrypTool is a software used to encrypt and decrypt messages. It provides an exciting insight into variety of ciphers, coding methods and analysis tools. It can be installed on machines. It has an online version which runs in the browser called CrypTool-Online (CTO). The CTO can be accessed by clicking on <https://www.cryptool.org/en/cto-ciphers> .

CTO has most of the ciphers that we have covered in the course. The questions that you have completed in the prior part, you should use those to double-check your answers using CTO.