

29/1/2019

B00093420 Eoin Finney

**Secure Communications**

**Labs 1-**

School of Informatics

Department of Informatics and Engineering

Technological University Dublin

Blanchardstown Campus

Dublin 15.

Bachelor of Science

Digital Forensics and Cyber Security

28/1/2019

# Lab 1 – Decoding Classic Cyphers

## Exercise 1: Rotational ciphers

1. The original Caesar cipher alwaYs used a shift of three
2. ROT 13 WAS USED BY MICROSOFT FOR ENCODING WINDOWS REGISTRY ENTRIES
3. COMMON VARIATIONS OF THE SHIFT ARE OFTEN USED LIKE DIFFERENT KEYS
4. THESE CIPHERS ARE TRIVIAL TO CRACK AND SOLVE EVEN BY HAND
5. With experience you will start to recognise the character sets of each encoding.

## Exercise 2: Substitution Ciphers

1. atbash cipher was a substitution cipher that reversed the alphabet
2. This is an example
3. frequency analysis is the key to breaking substitution ciphers the longer the message the easier it becomes

## Exercise 3:

aS suBStItUtIoN CIpHErs BECAME PoPuLAR, pEoPlE BEGAN TryING to

AttACk AND DECODE tHEM, AND tHE wEAKnEsSEs ASsOCIAtED wItH tHEM

stARtED To BECoME KnOwN, sEvErAL CIPHErs EMErGED wITH tHE sAME IDEA oF

tRyING tO BREAK THE EFFECTIvENEss OF FrEquENCy ANALySIs AND

HENCE MAkE tHE CIPHErS mOrE sECUrE. THE MAIn IDEA wAS tO COmE uP

wItH mEtHoD sO tHAT A PLAINtExt LEttER DIDN’t ALWAys MAP tO tHE SAME

CIPHErtEXt LETtEr (SyMBOl), to ACHIEvE tHIs tHE CIPHErS usED A

rEPEAtInG KEy. by FAr tHE MoSt wELl-KNOwN oF tHESE CIPHErS Is tHE

VIGENèrE CIpHEr BUt tHErE ARE MANy OtHErs WItH VEry SIMILAr

DEsIGNs.

## Exercise 4:

A TRANSPOSITION CIPHER ALSO CALLED COLUMNS PERMUTATION IS A TECHNIQUE TO CHANGE THE ORDER OF THE LETTERS IN A TEXT BY PLACING IT IN A GIRD

# Lab 2b – Numbers Station

The message in original form:

66475 19274 92028 78494 24146 68542 17504 39398 32348 59378 70636

Using the one time pad (OTP) given, I added each number together and modded them by 10. The OTP was the following:

66153 77185 10800 54937 48159 83271 12892 07132 34987 53954 23074

By adding and modding, I ended up with this:

22528 86359 02828 22321 62295 41713 29396 36420 66225 02222 93600

After getting this, I ran it against my straddling checkerboard using AT-ONE-SIR as the key, getting this message:

DELIVER ALL DOCUMENTS TOMOROW BY DEAD DROP A

# Lab 7 – Extra Decoding Challenge

# Lab 8 – Simple Blockchain

Part 1 consists of print(‘Hello World’).

To calculate the hash of “Hello World”, I wrote a program that takes a string and hashes it to md5:

A screenshot of a cell phone

Description automatically generated