

29/1/2019

B00093420 Eoin Finney

**Secure Communications**

**Labs**

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

Table of Contents

[Info 3](#_Toc7991549)

[Lab 1 – Decoding Classic Cyphers 4](#_Toc7991550)

[Exercise 1 - Rotational ciphers 4](#_Toc7991551)

[Exercise 2 - Substitution Ciphers 4](#_Toc7991552)

[Exercise 3 – Vigenère cipher: 4](#_Toc7991553)

[Exercise 4 – Transposition Cipher: 4](#_Toc7991554)

[Lab 7 – Extra Decoding Challenge 5](#_Toc7991555)

[Lab 2b – Numbers Station 5](#_Toc7991556)

[Lab 10b – Analysing FTP traffic 5](#_Toc7991557)

[Lab 10c – Pcap Challenges 5](#_Toc7991558)

[Challenge 1 5](#_Toc7991559)

[Challenge 2 6](#_Toc7991560)

[Lab 11 – Digital Signatures 6](#_Toc7991561)

[Installed Certs 6](#_Toc7991562)

[Digital Signatures 7](#_Toc7991563)

[Lab 13a – SSL/TLS Security 7](#_Toc7991564)

[Lab 13b – Tor and the Darkweb 7](#_Toc7991565)

[Lab 14 – Tor Website 8](#_Toc7991566)

# Info

40 % = Submission of selected weekly labs

Must submit a single document containing a detailed write up for the 8 selected labs Selected labs are indicated in labs section with an (\*) Each lab is worth 5% (8 \*5 =40%) You need to submit any 8 the following 9 labs:

* Lab 1 - Decoding Classic Ciphers & Lab 7 -Extra Decoding Challenge (both together count as 1 lab)
* Lab 2b - Numbers Station
* Lab 6b - Salted Hashes
* Lab 10b - Analysing FTP traffic
* Lab 10c - Wireshark Challenges
* Lab 11a - Viewing Certs & Lab 11b - Exchanging Signed Docs (both together count as 1 lab)
* Lab 12 - Encrypted Wireless Capture
* Lab 13a - Securing Internet Traffic & Lab 13b - Tor and the Dark Web (both together count as 1 lab)
* Lab 14 - Make your own TOR website.
* Tor Due date: Sunday 5th May @ midnight Bonus: You can choose to take part in the Zero Days CTF event in place of any two labs.

Labs taken place with ZeroDays:

* 6b - Salted Hashes
* 12 - Encrypted Wireless Capture

# Lab 1 – Decoding Classic Cyphers

In this lab, I was tasked with solving some classic ciphers

## 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 – Vigenère cipher:

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 – Transposition Cipher:

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 GRID

## Lab 7 – Extra Decoding Challenge

Did not solve.

# 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 10b – Analysing FTP traffic

Not done.

# Lab 10c – Pcap Challenges

This lab challenged me to get particular things from two .pcap files. The first challenge was to get username and password login credentials, while the second challenge was to find the key to gain access to a secret party. The background information for this challenge goes as follows:

Some dude I know is planning a party at some bar in New York! I really want to go but he's really strict about who gets let in to the party. I managed to find this packet capture of when the dude registered the party but I don't know what else to do. Do you think there's any way you can find out the secret password to get into the party for me? By the way, my favorite hockey player ever is mario lemieux.

## Challenge 1

Username: csaw

Password: welcome to 1969

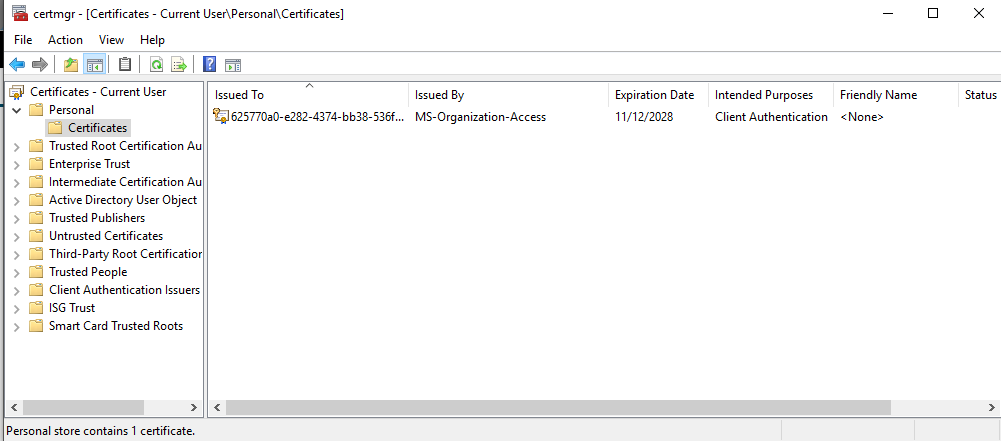
## Challenge 2

The party is being held at Taproom307. The secret phrase is “Brooklyn beat box”. Found in packet number 54755.

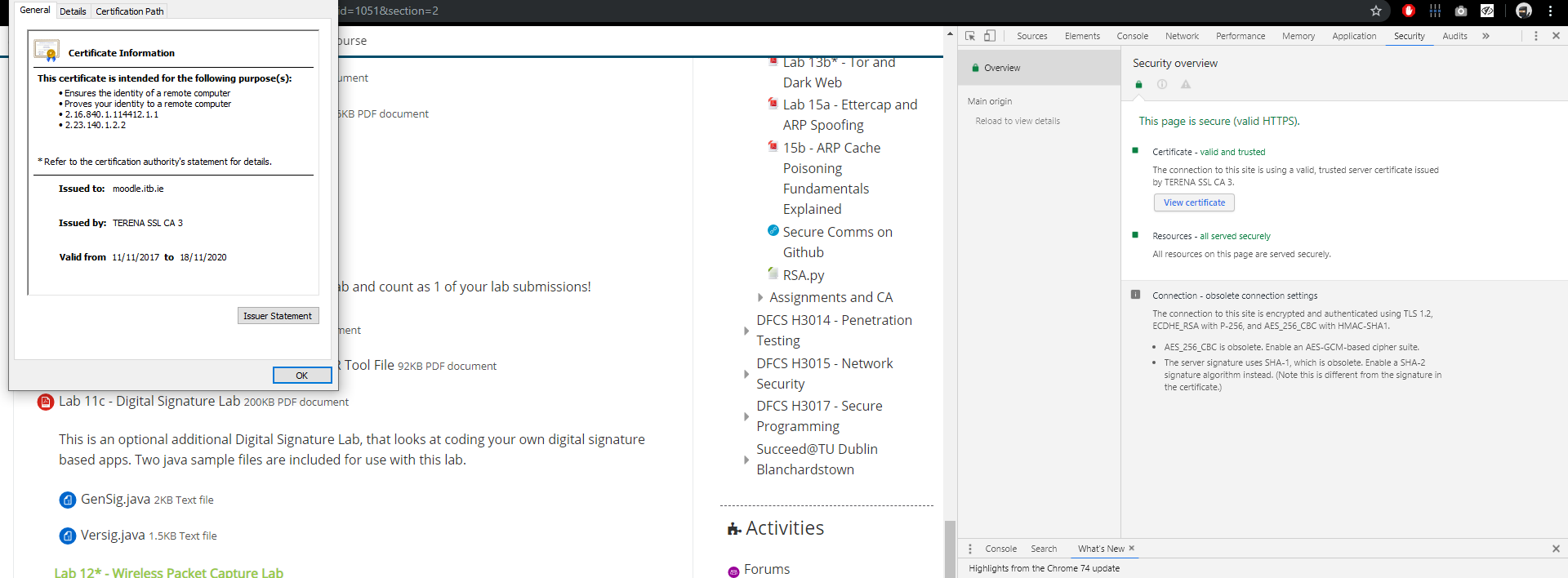
# Lab 11 – Digital Signatures

## Installed Certs

For this lab, I was tasked with the simple task of viewing digital certificates that are installed on my system (windows). To do this, I pressed the Win Key + R to open a run prompt, then typed certmgr.msc.



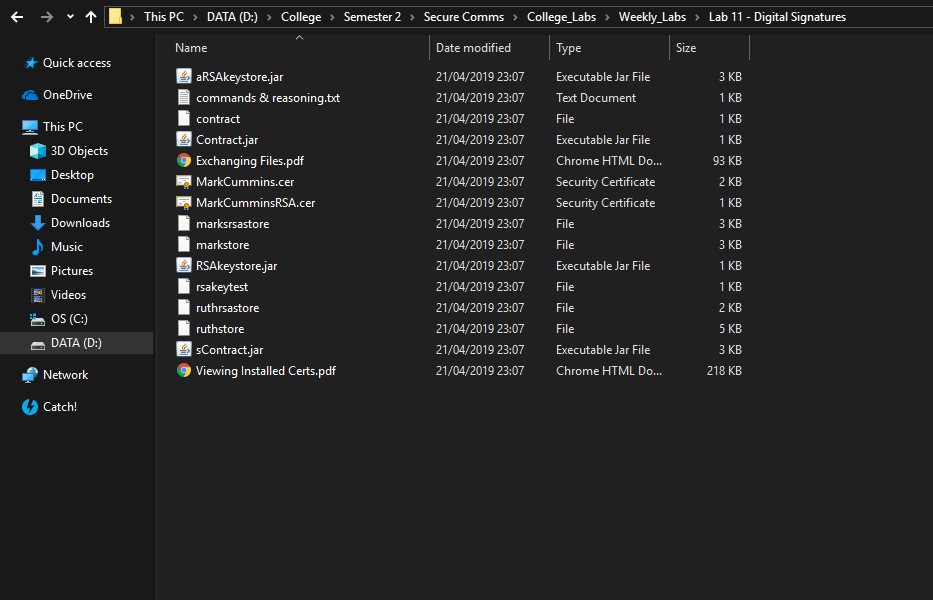
To view the certificate on the browser, I opened the browser, opened dev tools using Ctrl+Shift+I and the navigated to the security tab. To get the cert window open as show below, I pressed the view certificate button.



## Digital Signatures

Lab can be found at Github.com/Finneyyy

Following the steps written in the lab (Which is basically pretending to be Person1 and sending the digitally signed file to Person2, and then pretending to be Person2 and verifying that the file actually came from Person2), I ended up with a folder that looks like:



# Lab 13a – SSL/TLS Security

Not done

# Lab 13b – Tor and the Darkweb

Upon downloading the Tor Browser from the tor project (<https://www.torproject.org/>), the main install folder contains to items, a folder called Browser and a shortcut to start the Browser.

With my location being my home, whatsmyip.net tells me that my ip is 87.118.112.63, when my own starts with an 86 (eircom).

Looking up hidden wiki on ddg, I found a link to The Hidden wiki (http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main\_Page)

# Lab 14 – Tor Website

To do this lab, I used WAMP on windows 10, as WAMP has Apache2 (for the server built in). It is recommended to use thttpd as Apache2 has a habit of leaking IP addresses. Upon launching WAMP, I change the port used on Apache2 to 8080, then downloaded TOR (<https://www.torproject.org/>). Upon opening the folder, I click the shortcut for starting the browser to make sure it works, then close it. I then went into /Browser/TorBrowser/Data/Tor, and opened the ‘torrc’ file (which is basically the basic config file for the TOR Browser). To set the website up, I added to the bottom of the file 3 lines:

#Hidden Service

HiddenServiceDir D:\Program Files (x86)\TOR\Tor Browser\Browser\TorBrowser\Data\tor-service

HiddenServicePort 8080 127.0.0.1:8080

The first line is basically a comment for what comes next. The second line tells the browser where the service’s files are held (in a new folder called tor-service. This folder will contain the hostname of the .onion site and a private key). The third line tells the browser which port and what ip address the hidden service should run on.

The .onion link I received was this: tsomlpxnsvos3xan4ius5vhcmezdghd4bti6gcqui5wlyz3nyjnid4yd.onion