# 

# Advanced Security 1 Assignment

# Aileen Coliban

# 23/09/2025

1. In this part you will be required to list Cryptographic applications you will use to lock down the web browser you are using. In other words, how will you make your browser more secure, so that it mitigates the exposure of your personally identifiable information and any other data you may wish to protect? List the applications you will install in your browser to show who is tracking you. Why are you being tracked in every click you make? Is it possible to prevent being tracked? If yes, why or if no why not? Do not write more than one a page.

To make a web browser more secure and protect personal data, I would use a mix of cryptographic tools and privacy-focused extensions. The main goal is to reduce how much of my personally identifiable information leaks online and to make it harder for third parties to track what I’m doing.

First, I’d make sure that all my browsing traffic is encrypted. Tools like **HTTPS Everywhere** force connections to use TLS so data isn’t exposed in plaintext. This stops eavesdroppers or anyone on the same network from reading what I’m sending or receiving. On top of that, using a **VPN** can hide my IP address and add another layer of encryption, which makes tracking my location and activity more difficult. I would also rely on a **password manager** so that all my accounts have strong, unique and encrypted passwords which avoids the risk of data breaches.

For everyday browsing, I’d install extensions like **uBlock Origin** or **Privacy Badger** or both**.** uBlock Origin is a general ad and tracker blocker, but it also includes a logger tool that shows what domains are trying to connect in the background. While Privacy Badger detects and blocks third-party trackers that are tracking your activity, it also shows which third-party domains are trying to follow me across sites. **Ghostery** can also be used since it gives me a dashboard of the different ads, analytics tools and trackers running in the background. Most tracking comes from cookies and invisible scripts, so tools like **Cookie AutoDelete** help by clearing cookies automatically when I close tabs.

**Why are you being tracked on every click you make?**

Every click has commercial value. Companies use cookies, third-party scripts, and browser fingerprinting to build detailed profiles of a person’s habits. Advertisers want to know what you read, watch, or buy so they can target ads more effectively. Social media platforms track both on and off their sites to connect your browsing history with your identity. Even analytics tools built into websites contribute to this constant tracking.

**Is it possible to prevent being tracked?**

It’s not possible to completely prevent tracking but by combining encryption tools that have been stated above with privacy-focused extensions, I can lock down my browser enough to protect my personal information and stop most of the tracking. While total prevention isn’t realistic because some metadata always leaks, these tools greatly reduce the risks and keep my personal data far better protected.

2. Write a program that will implement Caesar Cipher. You can use Java or any other programming language. You can use online cryptographs tools (http://www.cryptool.org/en/) to check the accuracy of your programs. Please note that there are a lot of tools you may use to complete this part, just search on the Web.

A screenshot of a computer screen

AI-generated content may be incorrect.

A blue background with white text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

3. The following information was encrypted using Caesar Cipher. Using your own program, Decrypt it.

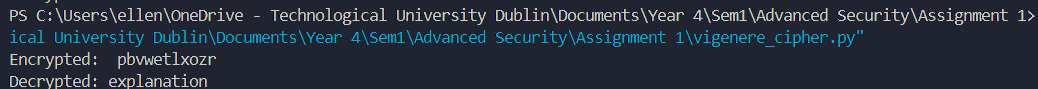
RQH YDULDWLRQ WR WKH VWDQGDUG FDHVDU FLSKHU LV ZKHQ WKH DOSKDEHW LV "NHBHG" EB XVLQJ D ZRUG. LQ WKH WUDGLWLRQDO YDULHWB, RQH FRXOG ZULWH WKH DOSKDEHW RQ WZR VWULSV DQG MXVW PDWFK XS WKH VWULSV DIWHU VOLGLQJ WKH ERWWRP VWULS WR WKH OHIW RU ULJKW. WR HQFRGH, BRX ZRXOG ILQG D OHWWHU LQ WKH WRS URZ DQG VXEVWLWXWH LW IRU WKH OHWWHU LQ WKH ERWWRP URZ. IRU D NHBHG YHUVLRQ, RQH ZRXOG QRW XVH D VWDQGDUG DOSKDEHW, EXW ZRXOG ILUVW ZULWH D ZRUG (RPLWWLQJ GXSOLFDWHG OHWWHUV) DQG WKHQ ZULWH WKH UHPDLQLQJ OHWWHUV RI WKH DOSKDEHW. IRU WKH HADPSOH EHORZ, L XVHG D NHB RI "UXPNLQ.FRP" DQG BRX ZLOO VHH WKDW WKH SHULRG LV UHPRYHG EHFDXVH LW LV QRW D OHWWHU. BRX ZLOO DOVR QRWLFH WKH VHFRQG "P" LV QRW LQFOXGHG EHFDXVH WKHUH ZDV DQ P DOUHDGB DQG BRX FDQ'W KDYH GXSOLFDWHV

ONE VARIATION TO THE STANDARD CAESAR CIPHER IS WHEN THE ALPHABET IS "KEYED" BY USING A WORD. IN THE TRADITIONAL VARIETY, ONE COULD WRITE THE ALPHABET ON TWO STRIPS AND JUST MATCH UP THE STRIPS AFTER SLIDING THE BOTTOM STRIP TO THE LEFT OR RIGHT. TO ENCODE, YOU WOULD FIND A LETTER IN THE TOP ROW AND SUBSTITUTE IT FOR THE LETTER IN THE BOTTOM ROW. FOR A KEYED VERSION, ONE WOULD NOT USE A STANDARD ALPHABET, BUT WOULD FIRST WRITE A WORD (OMITTING DUPLICATED LETTERS) AND THEN WRITE THE REMAINING LETTERS OF THE ALPHABET. FOR THE EXAMPLE BELOW, I USED A KEY OF "RUMKIN.COM" AND YOU WILL SEE THAT THE PERIOD IS REMOVED BECAUSE IT IS NOT A LETTER. YOU WILL ALSO NOTICE THE SECOND "M" IS NOT INCLUDED BECAUSE THERE WAS AN M ALREADY AND YOU CAN'T HAVE DUPLICATES.

A screen shot of a computer

AI-generated content may be incorrect.

4. Write a program that will implement Vigeneré Cipher. You can encrypt the word “explanation” using the key leg. You can use Java or any other programming language



5. Write a Java program (or any other programming language you are happy to use) to encrypt and decrypt plaintext using a 2 x 2 Hill cipher.

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.