ECE 458/750: Computer Security Final			Marks obtained ↓
Date: Aug 15, 2025	Total questions: **10**	Total points: **68**	
ID:	Name:		Time: 2.5 hrs

Page:	2	4	5	6	7	8	9	10	11	12	13	14	15	Total
Points:	8	9	5	4	4	2	7	4	4	9	3	4	5	68
Score:														

Instructions

No aids allowed. All you are allowed is a pen and pencil.

Use space provided. Answer the questions in the spaces provided. If you run out of room for an answer extra pages are provided at the end of the test booklet starting on page 16. They are clearly marked as EXTRA ANSWER SPACE. Please state in the original answer space if the extra pages are being used so that the grader knows to look there.

Point value in right-hand margin. The number of points each question is worth is listed in the right hand margin. The number of points and the space provided are roughly indicative of how long of an answer is expected.

Pencils and pens allowed. Both pens and pencils are allowed. Pencil marks need to be clearly present or erased. If it is unclear if a mark is or is not present then it is up to the discretion of the grader and this point cannot be contested later.

General Security Questions

1. Modify the following URL so that Amazon will sort the Train search in *ascending* order of price. (2)

   `https://www.amazon.ca/s?k=trains&s=price-desc-rank&ds=v1%3A2WgV5wtIVnK4FlQXU2U1DP`

   Solution: `https://www.amazon.ca/s?k=trains&s=price-asc-rank&ds=v1%3A2WgV5wtIVnK4FlQXU2U1DP`

   Any answer that makes it clear that the "s=price-desc-rank" part of the URL needs to be modified to something related to "ascending". Its ok if "asc" part is not exact, but URL reading and first-guess modification should be clear.

2. If you were to enter the following URL into a browser what website would the browser attempt to visit? (Note the URL is fake and will result in an error, but the browser will still attempt to find the IP Address associated with a site.) (2)

   https://regionofwaterloo.ca@uwaterloo.ca/electrical-computer-engineering/instagram.com

   - ◯ Region of Waterloo
   - ◯ Canada Government
   - ◯ University of Waterloo
   - ◯ Electrical and Computer Engineering for U. Toronto
   - ◯ Instagram

   Solution: University of Waterloo. Canada.ca is in the username position, amazon.ca is a path or a file, either way not a domain.

3. Which of the following best describes the Swiss Cheese Model used in computer security? (2)

   - ◯ A security architecture where multiple layers of defence are implemented, each with potential weaknesses, so that breaches only occur if the weaknesses in each layer align.
   - ◯ A vulnerability scanning technique that focuses on detecting holes in a single layer of security, similar to how cheese has holes.
   - ◯ A network segmentation approach where security devices are arranged in a circular pattern, forming a "cheese wheel" of protection.
   - ◯ A cryptographic method that uses randomly generated patterns with "holes" in the data to obscure sensitive information.

   Solution: *A security architecture where multiple layers of defence are implemented, each with potential weaknesses, so that breaches only occur if the weaknesses in each layer align.*

4. State a password that has high entropy but is easy to guess. (2)

Solution: P@ssw0rd1

Cryptography

5. (a) For each of the following statements, indicate if they are true (**T**) or false (**F**). (3)

_____ Caesar Cipher is vulnerable to frequency analysis.

Solution: T - Caesar cipher just shifts each letter around. So the most frequent letter in English, 'e', likely maps to the most frequent letter in the cipher text.

_____ A Playfair ciper is vulnerable to frequency analysis.

Solution: F - Playfair uses "blocks" of two characters. So there is some information diffusion and simply looking at the frequencies will not let an attacker know what a specific letter means.

_____ One-time-pad is vulnerable to frequency analysis.

Solution: F - A one time pad has the same key length as the message length. The key is added to the message (with a mod) to get the cipertext. Therefore a specifc letter in the message will not consistently map to the same letter in the cipher text.

(b) State one advantage of using a block cipher compared to a stream cipher. (3)

Solution: Information diffusion. Block ciphers move characters around (Double Transposition Cipher) and/or change them based on neighbouring characters (Playfair).

Immunity to insertion. If an attacker injects a character, the whole block decryption will fail, so we know that an injection occurred.

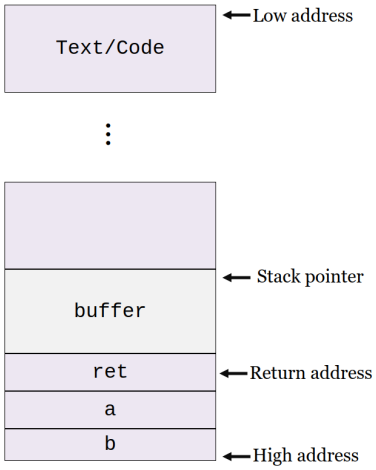
(c) State one advantage of using a stream cipher compared to a block cipher. (3)

Solution: Speed of encryption/decryption. Each character can be processed by itself, no need to wait for the other characters.

Error propagation. Each character is processed alone, independent of other characters so if there is an error in transmission it only impacts the one character.

Buffer Overflow

The following picture depicts a stack-smashing buffer overflow. The stack grows "downwards," while the buffer is written "upwards". The contents of the buffer therefore "smash" the stack.



6. In the third assignment you had to turn off *Address Space Randomization* in order to exploit the Buffer Overflow vulnerability. What would have happened if you had left *Address Space Randomization* on? Why would it have become incredibly hard to complete the assignment? (5)

Solution:

Session Hijacking

7. A website allows logged in users to change their passwords. The password-change page consists of only a new password box and a submit button. When "submit" is clicked the form sends the new password to the server. It also sends the cookie that contains an ID that states who the user is and proves that they are logged in. The code below executes on the server and processes the password-change request:

```
function change_password {
    user = get_logged_in_user(cookie_values[''user''])
    new_password = POST_values['new_password']
    new_salt = bcrypt.gensalt()
    hashed = bcrypt.hashpw(new_password, new_salt)
    database.update_user_password(user, hashed, new_salt)

    return ''Password updated!''
}
```

(The code is written in pseudocode for readability.)

The above code makes it possible for an attacker to engage in *session hijacking*.

(a) What is the code doing or not doing that makes session hijacking possible? (4)

> **Solution:** Session hijacking: If an attacker has access to a user's session (e.g., via XSS or stolen cookie), they can reset the password without knowing the old one. It removes one layer of protection: validating identity before changing critical credentials.

(b) Describe how the website software engineer could fix the above code (Question 7). Be specific, what would need to be changed and where would the change need to happen? (4)

Solution: The user should be asked to provide the current password. So the website needs to modify the form to include the current password. The server then should be sent the current and new passwords. The server should verify that the current password is correct. Then do the hashing + salt server-side and update the database there.

Verizon Supercookie

8. Verizon in this attack is a mobile phone carrier, phones with Verizon SIMs will send all their network traffic across the Verizon mobile network (unless WIFI is used). The Verizon Supercookie attack is a three part attack:

    - Verizon uses Man-in-the-Middle on Web traffic sent by their customers when using mobile data. The attack inserts a "X-UIDH: 15434" web header line in the web headers of HTTP connections. 'X' is traditionally used for custom headers. 'UIDH' stands for Unique Identifier Header and contains a unique number for each Verizon customer.
    - Any website can now view and record the inserted X-UIDH header information. If they are part of Verizon's partner program, they can also gain access to the user demographics associated with the X-UIDH value. This information allows them to provide targeted advertising to the user that matches their demographics.
    - The attack also enables third-party "zombie" cookies. A third party advertiser sets a normal cookie which they use for tracking (how trackers normally operate). If a user deletes the advertiser's cookie, the advertiser can then bring the cookie back by using Verizon's X-UIDH header value.

    Answer the following questions in regards to the Verizon Supercookie attack.

    (a) Where is the attack happening? Circle the best answer below: (2)

    ◯ Inside the mobile phone
    ◯ Inside the laptop
    ◯ WIFI access point (e.g. Coffee shop free WIFI)
    ◯ Internet Service Provider (ISP)
    ◯ Non-ISP Autonomous System (e.g. Akamai, Cloudflare)
    ◯ Destination web server

    Solution: ISP

(b) Explain why the Verizon Supercookie attack does not work over public WIFI access points like coffee shop free WIFI or airport free WIFI. (4)

Solution: The attack is being done by the mobile internet service provider (Verizon). If a free WIFI is used, then mobile data is not being used, and the path data takes through the Internet will likely not include the ISP. Man-in-the-middle only works if the attacker can get in the middle of the communication.

(c) A Verizon mobile customer Alice visits a set of pages S on her mobile phone, then she physically drives with her mobile phone to another town in the same USA state, after arriving she visits the same set of webpages $S' = S$ on her mobile phone. She did not have WIFI at either location. (3)

Would the Verizon Supercookie attack happen to both S and S' website visits? State 'yes' or 'no' and explain your reasoning.

Solution: Yes. Verizon is the mobile provider at both locations. Her physical location does not matter as long as she is still within Verizon's coverage range (whole USA according to them). So both the S and S' website visits would both be attacked the same.

(d) Describe how a third-party tracker, such as DoubleClick, can link the content of HTTPS website visits with the uniqueid information available from Verizon on HTTP website visits. (4)

Solution: The third party tracker is normally using their own tracking cookie AND the uniqueid provided by Verizon. When the user visits an HTTPS site, Verizon can no longer MITM the connection and the uniqueid value will not be inserted. But the cookie value previously sent by the tracker will still be sent. All the tracker needs to do is lookup the cookie value in their database and they are able to get the uniqueid and all the associated demographic data.

(e) The use of Supercookies by Verizon was investigated and found to break United States regulations. What about the attack violates how the United States manages Privacy? (4)

Solution: No information about the attack appeared on Verizon's privacy policies. The user also had no visibility and no control. In other words there was no notice and there was no choice. The US FTC views such cases as unfair and deceptive trade practice.

Lenovo Superfish

9. Lenovo is a company that sells laptops. Like most laptop companies Lenovo pre-installs their laptops with an operating system and some starter software. In this case, they decided to pre-install Superfish which is advertising software that injects ads into web pages the user is viewing. Even HTTPS protected websites.

   Superfish installed a self-signed root certificate on the Lenovo computer. It then sets up a proxy to direct network traffic through Superfish's software. Using the new root certificate, Superfish was able to Man-in-the-Middle attack all traffic. It used this ability to modify websites to add advertisements to its own preferred partners.

   (a) Where is the attack happening? Circle the best answer below: (2)

   - ◯ Inside the mobile phone
   - ◯ Inside the laptop
   - ◯ WIFI access point (e.g. Coffee shop free WIFI)
   - ◯ Internet Service Provider (ISP)
   - ◯ Non-ISP Autonomous System (e.g. Akamai, Cloudflare)
   - ◯ Destination web server

   Solution: It happens inside the user's computer. In the OSI model somewhere in 5-3.

   (b) For each of the following statements, indicate if they are true (**T**) or false (**F**) for a Lenovo laptop running Superfish. (4)

   _____ Superfish can read all communications sent to the user's banking website.

   Solution: T - Superfish can read all pages, including https protected ones.

   _____ Assuming a user logs into their bank using a username/password. Superfish can read financial account numbers displayed by the page, even when they are displayed on websites partially hidden, for example: "******123".

   Solution: F - Superfish cannot reach into databases. It can only see what servers send it.

   _____ Superfish logged keystrokes that users entered on all programs.

   Solution: F - It was only Man-in-the-Middle of network traffic.

   _____ Removing the Superfish application but leaving the root certificate installed would still leave the system vulnerable to Man-in-the-Middle attacks.

   Solution: T - Because the same private key was used for all installations and it was badly stored. Anyone with that private key (aka everyone) can perform a man-in-the-middle attack on the laptop as long as the self-signed root certificate is there. Superfish's software is not necessary.

   (c) Why is Superfish a Man-in-the-Middle attack? (3)

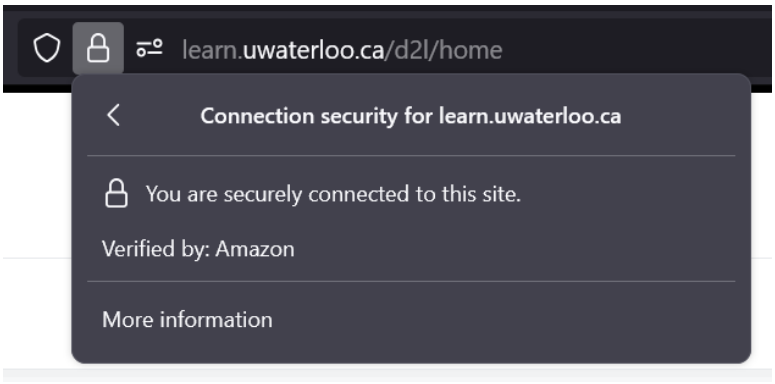


Figure 1: Connection security interface on Firefox when visiting the University of Waterloo Learn page.

(d) Figure 1 shows the lock icon and information dialogue that appears on Firefox when visiting University of Waterloo's Learn website. The image was taken in 2025 from a Microsoft Surface laptop. Imagine that a Lenovo laptop that had Superfish installed tried to take the same screenshot on the same website. What information in the image would be different? (3)

Solution: "Verified by: would change from "Amazon" to whatever name Superfish decided to add to their certificate, possibly "Superfish".
The "You are securely connected to this site." would not change.

(e) Imagine a correctly-implemented end-to-end encrypted chat app, like WhatsApp or Signal, that lets users verify their chat partner's public key. (Think about the verification activity.) Could Superfish read messages sent by such apps? State 'yes' or 'no' and explain your answer. (4)

Solution: No. They use public/private key cryptography directly without relying on Certificate Authorities. Instead a central server stores and manages the keys.

Onion Routing

10. Onion routing is built to ensure that a user's IP address cannot be associated with the traffic they are sending. It does this by sending traffic through several *nodes* before sending it across the open internet. (5)

    Onion routes are initially setup using public/private key cryptography but after setup the web traffic is encrypted using symmetric cryptography. Why are public/private keys not used for sending the web traffic?

Solution: Several reasons:

- Speed. Public/private is slower than symmetric (not well covered in class).
- One-session keys. Public/private keys are kept for long time frames and are more subject to loss. A symmetric key can be shared and used for just this session and then deleted.
- To keep confidentiality of the client node. This way traffic can go back along the onion route without giving away the identity (public key) of the client.

Extra Answer Space

If you need extra space to give an answer, please state in the original answer space that you will be using the extra pages and continue or write your answer here. If you choose to use the extra space as scratch paper, please write "scratch" so that graders know to ignore anything you have written.

EXTRA ANSWER SPACE

EXTRA ANSWER SPACE