ECE 458/750: Computer Security Midterm			Marks obtained ↓
Date: June 22, 2026,	Total questions: **24**	Total points: **73**	
ID:	Name:		Time: 75 minutes

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 19. 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.

Fill in or circle multiple choice answers. Multiple choice and multi answer questions will have boxes or circles next to the answer options. You may fill these in, clearly mark them, or circle the whole answer. It needs to be clear which answer option(s) have been selected.

Figures provided. Some content has been provided from the lecture slides. This content appears as figures, and is directly referenced by the question were we expect that you will need the figure information. For example: "The rules on Figure 1 may be helpful in this question."

Solution: This version of the exam has solutions to the problems. The solutions presented here are one possible solution but for open-ended questions they may not be the only possible solution. The solutions also represent how the instructor originally intended the question to be interpreted. When marking, the instructor takes into account that students may interpret questions differently than intended which may alter the correct answers.

POST MARKING NOTES: While marking the exam we take note of common student confusions and unanticipated issues with how students interpreted exam content. Boxes marked "POST MARKING NOTES" contain comments from the Instructor or TAs about how we handled some of the more common cases.

General Security Questions

1. In the definition of security, what do the letters CIA stand for? Fill in the blanks below. (3)
   C _____

   I _____

   A _____

> **Solution:** Confidentiality, Integrity, Availability.
>
> Full marks for the A being Accountability or Authentication. Technically not CIA, but still part of the definition.

2. 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.*

3. How does threat modeling help in selecting appropriate security protections for a system? (2)
   - ◯ By ensuring all possible security controls are implemented regardless of cost
   - ◯ By focusing only on protecting against known past attacks
   - ◯ By identifying specific threats and choosing defences that directly address those threats
   - ◯ By eliminating the need for security testing after development

> **Solution:** By identifying specific threats and choosing defences that directly address those threats

4. Which of the following is an example of multi-factor authentication? (2)
   - ◯ Entering a password twice
   - ◯ Using a password and answering a security question

◯ Using a password and a one-time code from a mobile authenticator app

◯ Logging in with a username and password

Solution: Using a password and a one-time code from a mobile authenticator app

Multi-factor authentication measn two of: something you know, something you have and something you are.

Access control and authentication

5. Which statement best explains how 2-factor authentication increases the security of password-based authentication? (2)

   ◯ It requires the user to provide multiple factors that have different security limitations.

   ◯ It limits the number of login attempts a user can make.

   ◯ It stores passwords in a more secure database format.

   ◯ It makes passwords longer and harder to guess.

   ◯ It prevents phishing attacks entirely by verifying the authenticity of websites.

   Solution: It requires the user to provide multiple factors that have different security limitations.

6. Imagine you were logged into a website, such as the uwaterloo.ca site, and wanted to force a logout. Which of the following approaches would work? (Select all that apply.) (2)

   ☐ Delete the session cookie

   ☐ Replace the session cookie value with random characters

   ☐ Close the browser and manually open the page again without modifying cookies

   ☐ Hard-refresh (clear cache) the page

   ☐ Disconnecting from the internet (e.g., turning off Wi-Fi)

   Solution: *Delete the session cookie* and *Replace the session cookie value with random characters*

   Closing the browser and disconnecting from the internet will temporarily make the page unavailable but not log the user out.

7. Linux both salts and hashes all passwords by default. State the threat model that salting and hashing is meant to protect against. How does having passwords hashed and salted protect against that threat model? (4)

   Solution: *Threat Model:* Offline guessing attack. Our threat mode assumes that the attacker has enough access to the server to obtain the password hashes and salts.

   Salting and hashing is intended to protect against an attacker that is able to get access to the password file (i.e. shadow file). It is effective because it increases the time/work the attacker needs to spend to guess each password. Because of the attacker must brute force guess each password individually and cannot use pre-computed hashes (rainbow tables).

8. Websites often rate limit password guesses so that only a small number of password attempts can be made sequentially. State the threat model that rate limiting meant to protect against. How does rate limiting reduce the risk of that threat? (4)

Solution: Threat model: Online attack where the attacker is limited to guessing passwords via the website. They are likely remote and have no access to hashed passwords.

How reduces risk: Rate limiting is effective because it limits how many times they can guess a password. If obvious passwords are not allowed (i.e. "12345678") then the attacker will possibly take years to guess a password with an online attack. Essentially this is the "don't care region" of password strength. As long as a user's password is strong enough and rate limiting is used, an online attacker will not be able to guess it.

Solution: POST MARKING NOTES

Give users time to change their passwords - For an online attacker, rate limiting does not give users time to change their passwords. Think about what an online attack looks like, for the website it looks just like a user trying to log in, just like how they always look. There are three possible scenarios:

- Website detects lots of guesses on the account. The website might encourage or require the user to choose a stronger password, but rate limiting will not really give the user more time to do this, and assuming a reasonably strong initial password, the user will be safe for a long time. A skilled website will also send the user a special link and not allow any login till the password has been reset.
- Attacker correctly guesses the password - from the website's perspective the person logging in has the password and is an authorized user. So they do not warn the user, because its normal. So the rate limiting does not help the user change their password at all.
- Attacker guesses the password, and logs in. The Website realizes the login looks a bit odd and sends a "login from a new location" message to the user's email. The user may then decide to change their password, but again, the rate limiting does not give them more time.

9. Online services often face password brute-force attacks from malicious actors. Describe how an attacker might conduct a brute-force password attack against an online authentication system. In your answer, discuss the different strategies attackers may use (e.g., simple brute force, dictionary attacks), the limitations and challenges they face, and the types of system weaknesses that make such attacks more feasible. Feel free to use the password game you played for the assignment when answering. (6)

Solution: This question was meant to test if you had played and understood the password game. OR just generally understood how password attacks happen. Many answers are possible here, below is a sample.

An attacker facing an online system would likely start by examining the website to understand how it submits passwords. They would then write a script (or use a tool) that allows them to automatically

submit the passwords rather than typing them into the website themselves. If the website has a rate limiting lockout, the script would likely be modified to submit passwords slowly for each user being attacked to avoid triggering the lockout.

The script would likely use a dictionary of known passwords that have been sorted by how commonly chosen they are. A brute force guessing of all combinations is unlikely to work in an online attack. But by starting with common passwords the attacker might get lucky that someone has used that password. Better yet, if they have a databased of leaked username/password combinations from another website, having the script try those would be much more likely to work.

The largest limitation is rate limiting by the website as it limits the number of guesses that can be tried in a short time frame, slowing down the attack. If all attacks come from the same IP address, there is also a risk the admin might notice and block the attacker's IP.

Weaknesses that might make an online attack more feasible involve poor decisions by the website developer. For example: error messages that contain hints. Helpful warnings about how a particular username does not exist in the system lets the attacker avoid wasting time guessing passwords for it. If the admin password is a standard default one, that is also a weakness that would help the attacker. Or if the website does something silly like require users to have 4 character passwords.

10. Advertisers use cookies to "track" usage habits across multiple website visits. Such tracking can be stopped by requesting an opt-out cookie. In theory, could a user set multiple opt-out cookies without visiting cookie opt-out sites? (2)

- ◯ Yes — by manually creating or editing cookies in the browser's developer tools, a user could replicate the opt-out cookie without visiting the opt-out site.
- ◯ Yes — installing multiple browser extensions that block tracking will automatically generate opt-out cookies across sites.
- ◯ No — opt-out cookies can only be set by the specific websites that manage tracking, so visiting each site is required.
- ◯ No — browsers prevent users from setting cookies manually for security reasons, so opt-out cookies must come from the original site.
- ◯ Partially — a user could copy an opt-out cookie from one browser to another, but could not create new ones without visiting the opt-out pages.

Solution: Yes — by manually creating or editing cookies in the browser's developer tools, a user could replicate the opt-out cookie without visiting the opt-out site.

11. A large company is designing a secure system to manage confidential product designs, and they want to ensure that only employees with the appropriate high-level clearance can view sensitive design documents with the goal of ensuring confidentiality. Which multi-level security model is the best match for this situation? (3)

- ◯ Bell-LaPadula Model
- ◯ Biba Model
- ◯ Principle of least privilege
- ◯ Access Control Lists
- ◯ Clark-Wilson Model
- ◯ Access Control Matrix Model
- ◯ Role-Based Access Control (RBAC) Model

Solution: Bell-LaPadula model.

The question is focused on confidentiality. So while the problem specifies "view" it likely also means that prevention of copying of high-security documents is wanted. Confidentiality is what the Bell-LaPadula model is about.

Cryptography

12. If my goal is information diffusion, which of the following ciphers should be used? (2)

- ◯ Caesar Cipher
- ◯ Vigenère Cipher
- ◯ Double Transposition Cipher
- ◯ Playfair Cipher

Solution: Playfair Cipher

This is the only block cipher on the list where information is diffused between letters. Double Transposition Cipher is a block cipher, but it just rearranges letters and does not diffuse information between them.

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

Solution: Information diffusion is normally the advantage for most, though not all, block ciphers. Block ciphers encrypt characters based on their and their neighbour's content. Playfair is a good example where the block size is 2, but changing either character in the 2 block will also impact the other character. A weaker example is Double Transposition Cipher where characters are re-ordered based on their position relative to their neighbours, but the diffusion here is very limited because only the position is changed, not the characters.

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

Solution: POST MARKING NOTES
Many people said that block ciphers are immune to insertion. I think my slides say this so we did not take points off. Technically insertion is possible with any cipher, it is just very visible with block ciphers. So technically the correct answer is that insertion is easy to detect in a block cipher.

Several answers said that frequency analysis is easier on stream than block ciphers. This may be true for Playfair vs Ceaser ciphers. But it is not necessarily true for Playfair vs Vigenere ciphers where the stream cipher key is being repeated. It is definitely not true for one time pads which are technically a stream cipher.

14. Select the phrase that best completes the statement: "A Playfair grid is constructed by" (2)

- ◯ arranging all 26 letters of the alphabet into a 5×5 grid by removing Q and keeping duplicate letters from the keyword
- ◯ inserting a keyword into a grid and then repeating the keyword until all cells are filled
- ◯ constructing a 5×5 grid using only the most frequent letters in English, followed by less frequent letters
- ◯ placing letters into a 5×5 grid based on their positions in the ASCII table

◯ placing a keyword into a 5×5 grid while preserving letter order, merging I/J, omitting duplicates, and then filling remaining spaces with unused letters in alphabetical order

Solution: placing a keyword into a 5×5 grid while preserving letter order, merging I/J, omitting duplicates, and then filling remaining spaces with unused letters in alphabetical order

15. Which of the following assumptions are required for cryptographic systems to ensure confidentiality and integrity? (Select all that apply.) (3)

- ☐ Encryption algorithms must remain secret for security to hold
- ☐ Only both communicating parties have access to the symmetric key
- ☐ Only both communicating parties have access to the private asymmetric key
- ☐ The private key in an asymmetric system is known to only one party
- ☐ Only one party needs to protect the symmetric key
- ☐ Public keys must remain confidential
- ☐ Attackers cannot intercept messages on the network
- ☐ Attackers must not know which algorithm is being used
- ☐ Only parties with the correct keys can successfully decrypt or verify protected data
- ☐ The system must hide all encrypted messages from the network entirely

Solution:

- Only both communicating parties have access to the symmetric key
- The private key in an asymmetric system is known to only one party
- Only parties with the correct keys can successfully decrypt or verify protected data

Solution: POST MARKING NOTES

Attackers cannot intercept messages on the network - Cryptographic approaches normally assume that messages may be intercepted and read when sent. If we could assume that messages cannot be intercepted then cryptography would not be needed.

Public keys must remain confidential - Public keys are meant to be shared widely. We assume that all people have access to it. Public/private key cryptography would not work if the public key was kept confidential.

3rd and 4th answers were combined - The third and fourth answers involving asymmetric private keys were treated as the same while assigning points. They were still given an X on Crowdmark if they did not match the solution above, but points were not deducted. It was clear that students confused the two answers because while only one person should ever have access the private key in asymmetric encryption, a communicating pair would each have access to their own private keys. The incorrect answer option does state "the private asymmetric key" suggesting that both people have access to the same asymmetric private key (which is bad security) but correct interpretation requires recognizing the significance of the word "the", and this is a security test, not an English test.

16. Use the Ceaser cipher to encrypt the plaintext message below. You may use Figure 1 if it is helpful. (4)
Key: 4 (a→e)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Figure 1: The above figure is scratch space. Marks made on this figure, or in the white space between the figure and this caption, will be ignored by the graders.

Plaintext: POND

Ciphertext: _____

Solution: TSRH

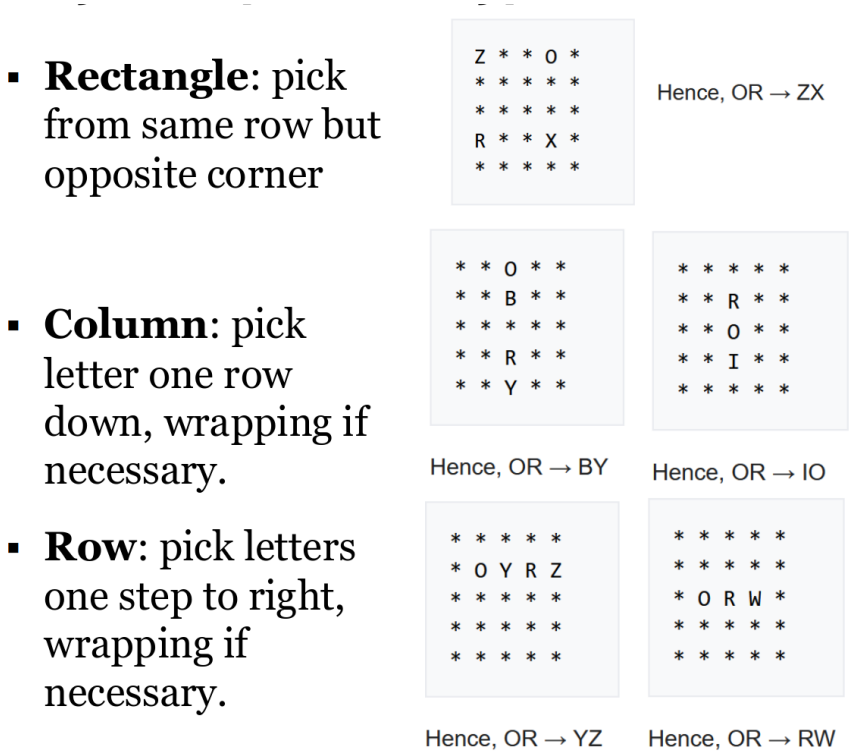


Figure 2: Rules for encrypting with Playfair

17. Use the following Playfair grid to encrypt the plaintext message. You may find the Playfair encryption rules in Figure 2 helpful. (4)

F	I	Z	B	U
A	C	D	E	G
H	K	L	M	N
O	P	Q	R	S
T	V	W	X	Y

Plaintext: HOTPOT

Ciphertext: _____

Solution: OTVOTF

Public/private key cryptography

18. Fill in the blanks in the following text describing Alice and Bob correctly communicating securely. Each blank needs to be filled in using one of the following words. The words can be used more than once and not all words need to be used: (6)

    - Encrypt, encrypted, encrypts
    - Decrypt, decrypted, decrypts
    - Sign, signed, signs, signature
    - Public
    - Private

    When they last met in person Alice and Bob verified and then _____ each other's _____ keys using their respective _____ keys.

    Later after they have gone home, Alice decides to send an encrypted email to Bob. Alice first _____ the message using her _____ key and then _____ the resulting message using Bob's _____ key. Alice then sends the message normally using a potentially untrusted connection.

    Bob receives the message and first _____ it using his _____ key. He then verifies that the message really was from Alice by verifying the _____ using Alice's _____ key.

    Solution: When they last met in person Alice and Bob verified and then **signed** each other's **public** keys using their respective **private** keys.

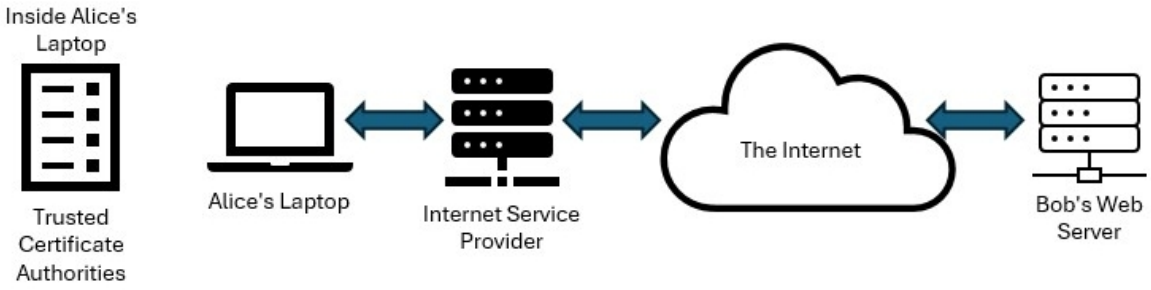
    Later after they have gone home, Alice decides to send an encrypted email to Bob. Alice first **signs** the message using her **private** key and then **encrypts** the resulting message using Bob's **public** key. Alice then sends the message normally using a potentially untrusted connection.

    Bob receives the message and first **decrypts** it using his **private** key. He then verifies that the message really was from Alice by verifying the **signature** using Alice's **public** key.

19. Certificate Authorities are intended to solve the problem of linking identities to public keys. How does using a Certificate Authority make encryption more scalable and reliable than the interaction described in Question 18? (4)

    Solution: A CA replaces the step where Alice and Bob have to sign each other's public keys using their private keys. Instead a CA certifies their identity on their behalf. Using a CA makes the process more scalable because users do not have to individually verify each organization they interact with, they only need to trust the CA to do the verification.

Man-in-the-middle



A Man-in-the-Middle (MITM) attack occurs when an attacker intercepts communication between two parties with the goal of reading and/or modifying content. Above is a simple diagram of Alice's laptop accessing a website. The traffic flows across Alice's Internet Service Provider (ISP), over the Internet, and finally reaches Bob's web server.

20. Which of the following entities could realistically perform a MITM attack on the above depicted connection if they wanted to? Assume the connection is not encrypted and that none of the computers are being accessed by non-authorized people. (Select all that apply.) (3)

- ☐ Alice's Internet Service Provider (ISP)
- ☐ Someone using the same ISP as Alice
- ☐ A router somewhere on the Internet path
- ☐ A random person with no access to the network path
- ☐ Alice's mobile phone which is not acting as a WIFI hotspot
- ☐ Anyone who knows the website's public URL
- ☐ Devices physically located in the same city as Alice
- ☐ A network filter program Bob intentionally installed on Bob's webserver

Solution:

- Alice's Internet Service Provider (ISP)
- A router somewhere on the Internet path
- A network filter program Bob intentionally installed on Bob's webserver

Solution: POST MARKING NOTES

Someone using the same ISP as Alice - this answer was ignored when assigning points. A surprising percentage of the class marked this answer, we think they had an incorrect interpretation that the "someone" might be an employee using ISP equipment, when we intended it to mean another user/client of the ISP. As the difference was unclear, we did not deduct points for tick marks on this answer.

- Another person using the same ISP (Internet Service Provider) cannot perform a MITM attack without first compromising some other computer such as the ISP's router. Traffic does not flow to all clients of an ISP natively.

Alice's mobile phone which is not acting as a WIFI hotspot - Alice's mobile phone is not part of the connection and will not see the network traffic at all. A phone-based attack will not work if it is not on the path the internet traffic is taking.

A network filter program Bob intentionally installed on Bob's (correct answer) - If Bob intentionally (authorized) a program on his server to filter (look at) internet traffic, then it can look at internet traffic and is therefore able to perform a MITM attack. MITM attacks do not need to be outside of a computer, they can also happen within the computer's software stack.

21. In Diffie-Hellman key exchange, computing exponentiation modulo a large prime is easy, but reversing the process (finding the exponent) is computationally difficult. This property is best described as: (2)

- ◯ Collision resistance
- ◯ Trapdoor function
- ◯ Perfect secrecy
- ◯ Redundancy
- ◯ Principle of least privilege

Solution: Trapdoor function

A trapdoor function is one that is easy to compute, but computationally expensive to reverse.

22. In a Diffie-Hellman key exchange, information is sent unencrypted between two parties, meaning a man-in-the-middle (MITM) attack is possible. What could a MITM attacker do during a key exchange? (Select all that apply.) (3)

- ☐ Intercept the public values sent by Alice and Bob
- ☐ Replace Alice's public value with the attacker's own value
- ☐ Establish separate shared keys with Alice and Bob without them realizing
- ☐ Directly compute the final shared secret key from intercepted values alone
- ☐ Relay the unencrypted messages unchanged without being detected
- ☐ Modify messages so that Alice and Bob derive different shared keys

Solution:

- Intercept the public values sent by Alice and Bob
- Replace Alice's public value with the attacker's own value
- Establish separate shared keys with Alice and Bob without them realizing
- Relay the unencrypted messages unchanged without being detected
- Modify messages so that Alice and Bob derive different shared keys

Solution: POST MARKING NOTES:
The answer option "Directly compute the final shared secret key from intercepted values alone" is ambiguous and was not used for grading, Ticking this box or not ticking this box had no impact on the grade for the question.

The issue with the answer option is the word "intercepted" which could mean "message read in transit" (intended meaning) or it could be interpreted as "message edited in transit". If the second, then this answer option becomes close enough to "Modify messages so that Alice and Bob derive different shared keys" that a reasonable student might be confused.

Passkeys

Passkey systems rely on public/private key cryptography.

23. In a passkey-based authentication system, which statement is true about the public and private keys? (2)

- ◯ Both keys are stored on the server to simplify authentication.
- ◯ The private key is sent to the server during each login attempt.
- ◯ The public key is stored by the server, while the private key remains on the user's device.
- ◯ The public key must be kept secret from attackers.

Solution: The public key is stored by the server, while the private key remains on the user's device.

24. Explain how PassKey's design helps protect against phishing attacks and credential database breaches. (3)

Solution:
Phishing: The computer that is running PassKey links each device-generated keypair to a specific website (or other device) and only sends to that linked entity. This means it is impossible for the user or the computer to send credentials or even sign a challenge message from a site other than the one it is meant to be used for.

Credential database breaches: Because websites only store public keys, if those keys are lost, that is ok because they were public to start with.

Solution: POST MARKING NOTES

While public/private key pairs are used by PassKeys, these are the device-generated ones, not the ones used by Certificate Authorities or websites. PassKey relies on browser-based auth of CAs and does not itself check that a website identity is accurate. It does check that the URL (host name) is as expected though.

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