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 13. 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."

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 _____

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.

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

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

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.

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)

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)

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)

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 teh password game you played for the assignment when answering. (6)

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.

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

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

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

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

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.

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

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)
Plaintext: POND

Ciphertext: _____

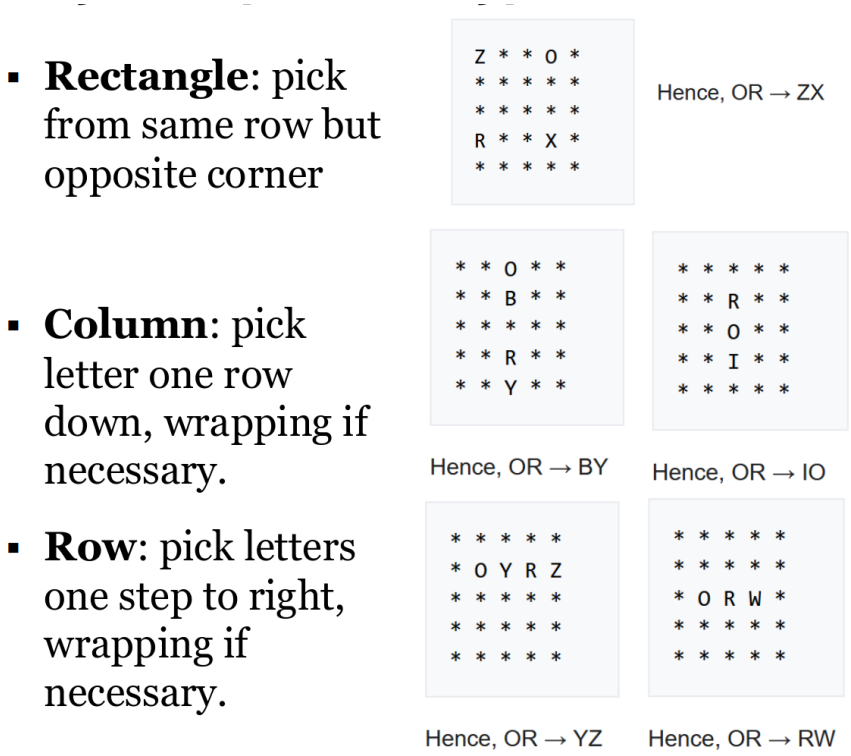


Figure 2: Rules for encrypting with Playfair

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: _____

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

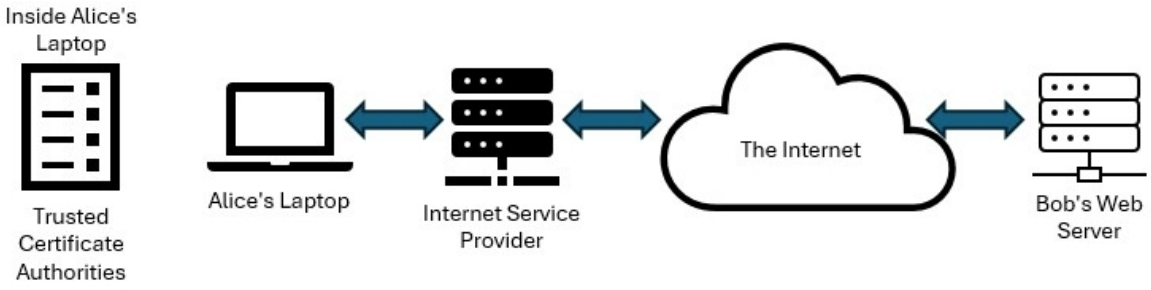
    When they last met in person Alice and Bob verified and then _____ each other's _____ keys using their respective _____ keys.

    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.

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)

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

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

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

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.

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

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