CSS454: Computer and Communication Security

Midterm Mock Exam

curated by The Peanuts

Name . . . . . ID . . . . . Section . . . . . Seat No . . . . . .

Conditions: Closed Book

Directions:

1. This exam contains 24 pages (including this one). If your exam has fewer, your paper has been subject to a *denial-of-service attack*.
2. Write your name and student ID clearly at the top.
3. This is a closed-book exam. No calculators, no dictionaries, no cheat sheets, and absolutely no neighbor's memory. Attempting to read someone else's answer is a *man-in-the-middle attack* and will be treated as such.
4. Answers must be written in English. Responses in Caesar-shifted Thai, Base64, or hexadecimal will not be graded.
5. Do not share answers with other students. Key reuse is a known vulnerability. Your answer is your private key, keep it that way.

For solution, ***click here****.*

Part I: True / False (10 points, 1 point each)

For each statement below, write **TRUE** or **FALSE** in the space provided.

1.1 _____ The CIA triad in information security stands for Confidentiality, Integrity, and Availability.

1.2 _____ Caesar Cipher is resistant to frequency analysis attacks because it uses multiple substitution alphabets.

1.3 _____ In Cipher Block Chaining (CBC) mode, each plaintext block is XOR-ed with the previous ciphertext block before being encrypted.

1.4 _____ Electronic Codebook (ECB) mode requires an Initialization Vector (IV) to function correctly.

1.5 _____ In RSA, a message is encrypted using the recipient's private key and decrypted using their public key.

1.6 _____ Elliptic Curve Cryptography (ECC) can achieve equivalent security to RSA with significantly smaller key sizes.

1.7 _____ In CP-ABE, the access policy is embedded inside the user's secret key SK_U rather than inside the ciphertext.

1.8 _____ OAuth 2.0 is primarily an authentication protocol that verifies the identity of a user.

1.9 _____ Among common biometric methods, iris scanning generally provides higher accuracy (lower false match rate) than fingerprint scanning.

1.10 _____ A digital certificate binds a public key to an identity and is digitally signed by a trusted Certificate Authority (CA).

Part II: Fill in the Blank (16 points, 2 points each)

Fill in each blank with the most appropriate term, value, or expression. Partial credit may be given for partially correct answers.

1. The general Caesar Cipher encryption formula is $C_i = (P_i + K) \text{mod}$ _____, where all values represent character positions in the English alphabet.

2. In RSA, the public key is represented as (e, n), while the private key is (_____, n). The security of RSA relies on the hardness of _____.

3. For n users communicating using symmetric encryption, the total number of keys required is _____ (Formula). For $n = 10$ users, this equals _____ keys.

4. In AES-CBC mode, the very first plaintext block is XOR-ed with _____ before encryption. This value must be _____ (secret / unpredictable / public) but should never be reused with the same key.

5. In CP-ABE, a user can successfully decrypt a ciphertext if and only if their _____ set satisfies the _____ embedded in the ciphertext.

6. OpenID Connect (OIDC) is an _____ protocol built on top of _____. The user identity information is returned in a _____.

7. In biometrics, the _____ Rate (also known as False Accept Rate) occurs when two biometric samples from different individuals are incorrectly judged to belong to the same person.

8. In hybrid encryption, _____ is used to encrypt the actual data (fast), while _____ is used to encrypt the session key (secure key exchange). This combination is often called _____.

Part III: Multiple Choice (30 points, 2 points each)

*Choose the **best** answer for each question. Circle or write the letter of your choice clearly.*

1. Which of the following is an example of a passive attack?

a) Modifying a transmitted message in transit

b) Replaying a captured authentication packet

c) Eavesdropping on network traffic without altering it

d) Launching a Denial-of-Service attack on a server

2. An organization disconnects its servers from the Internet to improve confidentiality. Which CIA property does this decision most directly sacrifice?

a) Confidentiality

b) Integrity

c) Availability

d) Authentication

3. The Vigenère cipher was designed to overcome a known weakness of the Caesar cipher. Which weakness does it specifically address?

a) The use of a symmetric key

b) Vulnerability to frequency analysis on single-character substitution

c) Inability to encrypt numbers and symbols

d) The key must be as long as the message

4. Which block cipher mode of operation produces the same ciphertext every time the same plaintext block is encrypted with the same key?

a) Cipher Block Chaining (CBC)

b) Electronic Codebook (ECB)

c) Counter (CTR)

d) Output Feedback (OFB)

5. AES-GCM is classified as an Authenticated Encryption with Associated Data (AEAD) scheme. What happens if the authentication tag verification fails during decryption?

a) The plaintext is released with a warning flag

b) Only the corrupted blocks are discarded; the rest of the plaintext is released

c) Decryption is rejected and no plaintext is released

d) The ciphertext is automatically re-encrypted with a new key

6. Which of the following cipher modes converts a block cipher into a stream cipher by encrypting successive counter values?

a) Electronic Codebook (ECB)

b) Cipher Block Chaining (CBC)

c) Counter (CTR)

d) Cipher Feedback (CFB)

7. Given RSA parameters $p = 3$, $q = 11$, $e = 3$, compute Euler's totient $\phi(n)$.

a) 30

b) 33

c) 24

d) 20

8. In hybrid encryption, why is RSA typically used to encrypt the session key rather than the entire message?

a) RSA produces smaller ciphertexts than AES

b) RSA is faster than AES for large data

c) RSA is computationally expensive; encrypting a small key is more practical

d) The session key must be stored in the RSA modulus n

9. The key advantage of ECC over RSA at equivalent security levels is:

a) ECC is based on integer factorization, which is harder than discrete logarithm

b) ECC requires significantly smaller key sizes, reducing computational overhead

c) ECC generates key pairs faster but verifies signatures more slowly

d) ECC does not use public-private key pairs

10. What security services does a digital signature primarily provide?

a) Confidentiality and availability

b) Confidentiality and integrity

c) Authentication and non-repudiation

d) Integrity and availability

11. A digital signature is created using:

a) The sender's public key

b) The recipient's public key

c) The sender's private key

d) The recipient's private key

12. In CP-ABE, which algorithm is called by the data owner to encrypt data and embed the access policy?

a) `Setup`(1^λ)

b) `KeyGen`(MSK, S)

c) `Encrypt`(PK, M, T)

d) `Decrypt`(CT, SK_U)

13. Consider the CP-ABE access policy `(doctor AND oncology) OR admin`. A user with attributes {`doctor, cardiology, manager`} attempts to decrypt. What is the result?

a) Decryption succeeds because the user is a doctor

b) Decryption succeeds because the user has the manager attribute

c) Decryption fails because the user does not satisfy the policy

d) Decryption succeeds using the collusion of manager and doctor attributes

14. What is the primary difference between OAuth 2.0 and OpenID Connect (OIDC)?

a) OAuth 2.0 is for authentication; OIDC is for authorization

b) OAuth 2.0 provides an ID token; OIDC provides an access token

c) OAuth 2.0 is for authorization (resource access); OIDC adds authentication (identity verification)

d) OAuth 2.0 uses JWT; OIDC uses XML-based SAML assertions

15. In OpenID Connect, what is the purpose of the `nonce` parameter included in the authorization request?

a) To identify the client application uniquely across requests

b) To bind the ID token to the client session and prevent replay attacks

c) To indicate the desired scopes for the access token

d) To encode the user's preferred language in the response

Part IV: Short Answer (40 points)

Answer each question clearly. Show all work for computation questions. Partial credit is awarded for correct reasoning even with a wrong final answer.

Question 1 (4 points)

Encrypt the plaintext **"CRYPTOGRAPHY"** using Caesar Cipher with key $K = 7$. Use the standard mapping $A = 0, B = 1, \ldots, Z = 25$, and the encryption formula:

$$C_i = (P_i + K) \bmod 26.$$

Show your computation for each character step by step and write the final ciphertext.

Question 2 (6 points)

Perform RSA key generation given the following parameters:

$$p = 3, \quad q = 11, \quad e = 3.$$

1. Compute n and $\phi(n)$.

2. Verify that $\gcd(e, \phi(n)) = 1$ and find the private key exponent d such that $de \equiv 1 \pmod{\phi(n)}$.

3. Using your public key (e, n), encrypt the message $M = 2$. Then verify by decrypting the resulting ciphertext back to M.

Question 3 (4 points)

Compute the following modular arithmetic expressions. Show your work; a bare answer receives no credit.

1. $(-17) \bmod 5$

2. $(-7) \bmod 3$

3. Find x such that $7x \equiv 1 \pmod{10}$. (Hint: try small values or use the extended Euclidean concept.)

4. $17^2 \bmod 11$

Question 4 (5 points)

Do you agree that "AES symmetric encryption alone is sufficient to secure data transmission between Alice and Bob over an untrusted network?" Support your answer by discussing:

- What AES provides (and does not provide),
- The key distribution problem,
- How hybrid encryption addresses this limitation.

Question 5 (6 points)

Explain the role of each of the following CP-ABE algorithms. For each algorithm, state: (a) who calls it, (b) its inputs, and (c) its output.

1. `Setup(`1^λ`)`

2. `KeyGen(`MSK`, `S`)`

3. `Decrypt(`CT`, `SK_U`)`

Question 6 (5 points)

A company's authentication system uses biometric recognition at its data centre entrance. The system is currently configured with a threshold that results in:

$$\text{FMR} = 0.1\% \quad \text{and} \quad \text{FNMR} = 8\%.$$

1. Define False Match Rate (FMR) and False Non-Match Rate (FNMR) in plain terms.

2. The security officer wants to reduce FMR to near zero. What trade-off will this cause? Explain the relationship between FMR and FNMR.

3. Suggest one biometric modality that provides inherently higher accuracy than fingerprint, and briefly justify your choice.

Question 7 (5 points)

Consider the CBC and CTR modes of AES operation.

1. A 128-bit block of plaintext P_1 = `0xABCD...` is to be encrypted. In CBC mode, what additional value must be XOR-ed with P_1 before the block cipher is applied? What is this value for the first block?

2. In CBC, if ciphertext block C_2 is corrupted during transmission, which plaintext blocks will be affected upon decryption? Explain why.

3. Why is CTR mode often preferred over CBC for random access decryption (e.g., seeking to a specific position in an encrypted file)?

Question 8 (5 points)

Compare OAuth 2.0 and OpenID Connect (OIDC) by answering the following:

1. A mobile fitness application wants to read a user's step count from Google Fit and display the user's name and profile picture after login. Which protocol(s) should the developer use for each requirement? Justify your answer.

2. In the OIDC Authorization Code Flow, what token is issued specifically to confirm the user's identity, and in what format is it typically encoded?

3. **Do you agree** that "OAuth 2.0 provides true user authentication"? Explain in 2–3 sentences why or why not.

Part V: Case Study (24 points)

Background Scenario: MedChain Hospital Cloud System

MedChain Hospital is building a **cloud-based patient record management system**. Patient records are stored on a semi-trusted cloud server operated by a third party. Multiple classes of users — cardiologists, oncologists, administrators, and insurance auditors — need to access records, but with **strictly different access rights**:

- **Cardiologists** may read records tagged as `cardiology`.
- **Oncologists** may read records tagged as `oncology`.
- **Administrators** may read all records.
- **Insurance auditors** may read only billing summaries tagged `billing`.

MedChain's security requirements are:

I. Patient data must remain **encrypted at rest** on the cloud server.

II. The cloud server must **not** be trusted with plaintext data.

III. Access control must be enforced **cryptographically** (not just by the server's access control list).

IV. Uploaded records must be **verifiably authentic** (i.e., the receiver can confirm who uploaded the record and that it has not been tampered with).

V. The system should support **physician login via a web portal** using Single Sign-On (SSO) without requiring separate credentials for each hospital sub-system.

Case Study — Question A (10 points)

The hospital's security architect proposes the following encryption scheme for uploading a cardiology record M:

(1) Generate a random AES session key k_{AES}.

(2) Encrypt the record: $CT_M = \texttt{Enc}_{AES}(k_{AES},\ M)$.

(3) Define an access policy:
$T =$ `(role = cardiologist AND dept = cardiology) OR (role = admin)`.

(4) Encrypt the session key: $CT_K = \texttt{Enc}_{CP\text{-}ABE}(PK,\ k_{AES},\ T)$.

(5) Upload $(CT_M,\ CT_K)$ to the cloud.

Answer the following sub-questions. Show full reasoning.

1. **(2 pts)** Write the full decryption procedure a physician with attributes $S = \{$`role=cardiologist, dept=cardiology`$\}$ must perform to recover M. Use proper notation, e.g. $\texttt{Dec}_{CP\text{-}ABE}(\cdots)$.

2. **(2 pts)** An oncologist with attributes $S' = \{$`role=oncologist, dept=oncology`$\}$ attempts to decrypt CT_K. Will this succeed? Justify using the access policy T.

3. **(3 pts)** Two users — Dr. Alpha (attributes: `role=cardiologist`) and Dr. Beta (attributes: `dept=cardiology`) — attempt to combine their secret keys to satisfy the policy T.

   (a) What is this type of attack called?

   (b) Does CP-ABE allow this? Explain briefly why or why not.

   (c) What is the technical mechanism CP-ABE uses to prevent it?

4. **(3 pts)** The hospital decides to switch from `AES-CBC` to `AES-GCM` for encrypting M.

   (a) What additional security property does AES-GCM provide that AES-CBC alone cannot?

   (b) In AES-GCM, what component is responsible for producing the authentication tag?

   (c) If an attacker flips a bit in CT_M during transit, what will happen when the recipient attempts to decrypt it with AES-GCM?

Case Study — Question B (8 points)

Requirement IV states that uploaded records must be verifiably authentic. The hospital architect proposes using **digital signatures**.

1. **(3 pts)** Describe step-by-step how a physician (sender) would digitally sign a patient record M before uploading it, and how the cloud audit system (verifier) would verify the signature. Your answer must specify:
   - Which key is used at each step,
   - The role of a hash function,
   - What a successful verification proves (and what it does not prove).

2. **(2 pts)** The cloud audit system must trust the physician's public key. Explain the role of a **Certificate Authority (CA)** and a **digital certificate** (X.509) in establishing this trust. What problem arises if a physician's private key is compromised?

3. **(3 pts)** The hospital now combines digital signatures and CP-ABE encryption. Write the complete protocol equations (encryption + signing) that a physician performs before uploading (CT_M, CT_K), and the equations that a verifier performs after downloading. Use proper notation.

Case Study — Question C (6 points)

Requirement V states that physicians should log in via SSO using a web portal. The hospital's IT team proposes using **OpenID Connect (OIDC)** on top of **OAuth 2.0**.

1. **(2 pts)** Briefly describe the OAuth 2.0 Authorization Code Flow (steps 1–5 are sufficient) as it would apply when a physician logs into the MedChain portal using their hospital identity provider (IdP).

2. **(2 pts)** The OIDC **ID Token** contains the physician's identity information.

   (a) In what format is the ID Token typically encoded?

   (b) List <u>two</u> claims that would be particularly useful for MedChain's access control system (beyond `sub` and `iss`).

3. **(2 pts) Do you agree** that OIDC alone (without CP-ABE) is sufficient to enforce MedChain's Requirement III ("access control must be enforced cryptographically, not just by the server")? Justify your answer in 3–5 sentences, explaining the fundamental difference between server-side access control and cryptographic access control.