CSCI1660/2660: Introduction to System Security (Spring 2026)
Midterm Exam

Instructor: Nikos Triandopoulos

March 12, 2026

Instructions

Please carefully read the following guidelines.

1. **Print your NAME and SIGN the exam at the bottom of the page.**
2. This is a closed-book exam, so you are allowed to use **no resources** while working on it.
3. The duration of the exam is **1 hour**.
4. You are bound by **Brown's Academic Code** and need to work on the exam **by yourself**.
5. Provide your answer to each question in the space provided after the question itself.
6. Be **brief and concise** in your written answers. No answer should take long to describe.

Good luck!

Your Full Name:

Your Signature:

Question 1 (20%)

(1.1) Consider the authentication server at Brown, storing passwords with which students, faculty and staff get access into any Brown-related resources and web services. Which of the security properties of the CIA triad become relevant for the protection of this server and why?

(1.2) When it comes to the design, standardization and wider adoption of cryptographic schemes, which approach is preferable in terms of security strength and societal benefit?

A. The design should make only accurate and realistic assumptions about an attacker's capabilities, because our society needs secure solutions to known vulnerabilities and existing threats.

B. Security through obscurity should be preferred, because fewer entities (e.g., only government agencies) know the underlying secrets, thus the less likely such secrets will leak to attackers.

C. Open design, public scrutiny and modern-crypto provable analysis by experts from academia, industry or agencies, are all vital for stronger security and better transparency in our society.

D. Schemes using public-key cryptography are strictly preferable, because they generally offer stronger security guarantees and they are accessible equally by all members in our society.

(1.3) What is a security control?

A. A security parameter (e.g., the length of a key) that controls how secure a crypto tool is.

B. A risk security analysis for optimally allocating limited resources under uncertain threats.

C. Specialized personnel who monitor computer system in order to detect possible cyberattacks.

D. A defense mechanism that protects against certain attacks and promotes a security property.

(1.4) The security goal behind the design of Message Authentication Codes (MACs) is to prevent any unauthorized manipulation of data. T F

Question 2 (20%)

(2.1) Explain how One Time Pad encryption works, what limitations render it impractical and why, and under which general framework and assumptions it is used in practice.

(2.2) The One Time Pad cipher is said to be perfectly secure. What does it mean?

A. That a given ciphertext can equally likely be the encryption of any message.

B. That brute force attacks are impossible even for small key sises.

C. That it is impossible to find two different messages that encrypt to the same ciphertext.

D. That once it is set up securely only one time, it is impossible to break for a lifetime.

(2.3) In which (0 to 4) of the following cases is One Time Pad securely used in practice?

A. Hybrid encryption.

B. Authenticated encryption.

C. CBC-MAC.

D. RSA encryption.

(2.4) The "hash & MAC" design paradigm currently relies on using the AES block cipher. T F

Question 3 (20%)

(3.1) In the cryptographic setting where a n-bit secret key is used in a scheme, how does computational security (for the scheme) relate to brute-force attacks (against the scheme).

(3.2) How do chosen-plaintext (CPA or "advanced") attacks differ than basic eavesdropping (EAV or "plain") attacks against a symmetric encryption?

A. A plain attacker learns only the ciphertext of any transmitted messages, whereas an advanced attacker also learns the plaintext that corresponds to some of the captured ciphertexts.

B. A plain attacker may attack a deterministic cipher, whereas an advanced attacker may attack either a deterministic or a randomized cipher.

C. A plain attacker is only curious to eavesdrop the communication and learn the plaintext, whereas an advanced attacker may also tamper with message transmissions.

D. A plain attacker has no additional help, whereas an advanced attacker obtains black-box oracle access to the (keyed) encryption algorithm.

(3.3) Which of the following (0 to 4) describe the importance of (pseudo)-randomness in security?

A. Secret keys should be not only be secret but also hard to predict.

B. Pseudorandom bit strings are necessary to achieve stronger security levels for encryption.

C. Cryptographic hashing relies on the availability of pseudorandom bit strings.

D. The security of many protocols relies on the use of random initial vectors, nonces or identifiers.

(3.4) By independently employing a deterministic block cipher for domain extension, the Electronic Code Book mode of encryption is susceptible to statistical analysis over the ciphertext. T F

Question 4 (20%)

(4.1) In a new browser tab you search for new service and sign up for it. Explain the security concepts related to the `https` and lock icon in the URL, and the 6-digit number texted to you.

(4.2) Intuitively, what is the birthday attack and what is its practical significance?

A. A birthday attack is a brute-force attack against ciphers, where candidate keys are randomly chosen, resulting in speedups for plaintext recovery by a factor of 2.

B. A birthday attack is a brute-force attack against cryptographic hash functions, where randomly chosen hash values are successively checked as candidate digests of randomly chosen pre-images, resulting in speedups for hash inversion by a factor of 2.

C. A birthday attack is a brute-force attack against cryptographic hash functions, where randomly chosen pre-images are successively hashed till a collision in the hash domain (of size 2^n) is found, o find collisions after only $2^{n/2}$ hashing effort.

D. A birthday attack is a brute-force attack against cryptographic hash functions designed by the Merkle-Damgård transform, to find collisions after only $2^{\sqrt{n}}$ hashing effort.

(4.3) To prove that she voted "right" in a Yes-No referendum, influencer Alice posts on Instagram the SHA2-512 digest of her secret vote. Which of the following (0 to 4) describe what happened?

A. Her vote remains secret because SHA2-512 evades birthday attacks.

B. She could have simply have posted her actual vote.

C. Her vote may or may not remain secret, depending on her account and browser settings.

D. She should have posted the digest of her vote prepended with a random value instead.

(4.4) Following the Merkle-Damgård design paradigm, SHA2 is state of the art in cryptographic hashing by supporting various secret-key or message-block sizes. T F

Question 5 (20%)

(5.1) How public-key cryptography compares to symmetric-key cryptography with respect to key management, assumptions, efficiency and security?

(5.2) How is a signature $(\mathsf{Sign}, \mathsf{Vrf})$ used to check the integrity of message m sent from S to R.

A. If $(\mathsf{PK_S}, \mathsf{SK_S})$ is the public-key pair of S, m is sent signed with signature $\sigma = \mathsf{Sign}(\mathsf{SK_S}, m)$, and received signed message (m, σ) is verified by checking whether $\mathsf{Vrf}(\mathsf{PK_S}, m, \sigma) = \texttt{accept}$.

B. If $(\mathsf{PK_S}, \mathsf{SK_S})$, $(\mathsf{PK_R}, \mathsf{SK_R})$ are the public-key pairs of R, S, m is sent signed with signature $\sigma = \mathsf{Sign}(\mathsf{SK_S}, m)$, and received signed message (m, σ) is verified by checking whether $\mathsf{Vrf}(\mathsf{PK_R}, m, \sigma) = \texttt{accept}$.

C. If $(\mathsf{PK_S}, \mathsf{SK_S})$ is the public-key pair of S, m is sent signed with signature $\sigma = \mathsf{Sign}(\mathsf{PK_S}, m)$, and received signed message (m, σ) is verified by checking whether $\mathsf{Vrf}(\mathsf{SK_S}, m, \sigma) = \texttt{accept}$.

D. If $(\mathsf{PK_R}, \mathsf{SK_R})$ is the public-key pair of R, m is sent signed with signature $\sigma = \mathsf{Sign}(\mathsf{PK_R}, m)$, and received signed message (m, σ) is verified by checking whether $\mathsf{Vrf}(\mathsf{SK_R}, m, \sigma) = \texttt{accept}$.

(5.3) Which of the following (0 to 4) can correctly refer to cross-site request forgeries?

A. The user connects to a malicious server that presented an invalid forged digital certificate.

B. The user executes a valid but unintended request to a web server to which they are logged in.

C. The user accidentally leaks their authentication cookie to the attacker allowing impersonation.

D. The user is trusted by the server, so unintended requests must be detected via random secrets.

(5.4) Replay attacks describe the threat wherein valid cryptographically signed messages, are maliciously altered and resent by the attacker, and verified by the receiver at a later time. T F