CSCI1660/2660: Introduction to System Security (Spring 2026)
Midterm Exam – Solutions & Rubric

Instructor: Nikos Triandopoulos

March 12, 2026

Instructions

Please carefully read the following guidelines on how to grade the midterm exam consistently.

1. Each Question X corresponds to **20 points** (20% of a total of 100 points) and consists of:
   - An essay subquestion X.1 corresponding to **7 points**.
     - An answer to X.1 is deemed as "Exemplary," "Adequate" or "Poor," and is awarded **7, 5 and 3 points**, respectively.
   - One multiple-choice question X.2 corresponding to **5 points**.
   - One multi-answer question X.3 corresponding to **5 points**.
     - If a correct answer is chosen then, starting with **5 points**, **1 point** is subtracted for each incorrect answer that is chosen. Otherwise, **0 points** are awarded.
   - One true-false question X.4 corresponding to **3 points**.
2. Any subquestion without an answer is awarded **0 points**.

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?

> **Answer:** All of the three properties become relevant: Confidentiality, because users' passwords need to remain secret and not leak to users or attackers breaking into the server; Integrity, because passwords need to remain correct or otherwise users are denied access or can be impersonated; and Availability, because if the authentication server becomes unaccessible then all Brown-related web services become also unaccessible (this is, for instance, what a ransomware attack achieves).
>
> - **Exemplary:** As above (essentially).
> - **Adequate:** Only two of the properties are identified as relevant and justified or all three properties are identified but are not justified.
> - **Poor:** Only one of the properties is identified as relevant and justified, or only two of properties are identified but are not justified.

(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.

> **Answer:** If the message space is n-bit strings, a random key k (or pad, or mask) of size n is chosen (and shared between Alice and Bob) and it is bit-wise XORed with the plaintext m to produce the ciphertext c, both of size n. Decryption of c into m works similarly by XORing again with k (since XORing with the k twice cancels out). The key is as long as the message and cannot be used twice, therefore the obvious approach to choose and securely share an n-bit key in order to protect only an n-bit message, makes absolutely no sense. Instead, OPT encryption is used in practice by deriving pseudorandom (random looking) bits out of the shared secret key k (e.g., using a PRG or PRF, i.e., a stream cipher or block cipher) and using these bits once as masks to transmitted masked messages. Perfect security becomes computational, meaning that the can only break the scheme by guessing the pseudo-randomness used, which will be infeasible for all practical purposes for efficient (polynomial time) attackers that have only negligible probability of success.
>
> - **Exemplary:** Essentially as above (all components are correct: encryption + decryption, 2 weaknesses + link to impracticality, key-derived pseudo-randomness + 2 assumptions).
> - **Adequate:** Some (1-3) elements are missing or described with mistakes.
> - **Poor:** One part or several (3+) elements are missing or described with mistakes.

(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).

> **Answer:** Computational security refers to the assumption that the scheme is attached by an adversary that is an efficient algorithm running in polynomial time in n and the assumption that we do not mind for negligibly small bad events. It relates to the two versions of brute-force attacks, namely exhausting key enumeration and random key guessing, by imposing that the attacker is unable to run for $O(2^n)$ time to brute force the secret key, and can at best guess the secret key with negligible probability $O(2^{-n})$, therefore, either brute-force strategy becomes not practically relevant for appropriate key sizes, e.g., 128, 256 or more.
>
> - **Exemplary:** Essentially as above.
> - **Adequate:** Explanation is in the correct direction but too vague or less accurate.
> - **Poor:** Explanation is partially incorrect.

(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.

> **Answer:** The lock icon corresponds to your browser certifying the identify of the connecting web server, through the verification of a public-key certificate, i.e., using the public-key of a known CA to verify the signature by this CA on a certificate linking the identity (e.g., URL) of the server to an identity description an a public key of this server. The `https` corresponds to using this verified public-key for your browser to use hybrid encryption in order to establish a secure sessions between the client and the server (e.g., using authenticated encryption, under a secret key chosen by the client and shared with the server using public-key encryption using the verified public-key of the server). The 6-digit number corresponds to the so-called 2nd factor authentication technique, where something the user possesses (their cellphone/device that has access to the registered mobile phone number) is used to provide more assurance about the authenticity of the user, beyond the something you know factor (e.g., in this case likely the password).
>
> - **Exemplary:** Essentially as above.
> - **Adequate:** One part is too vague or less accurate or incorrect.
> - **Poor:** Two parts are too vague or less accurate or incorrect.

(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, to 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.**

(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?

> **Answer:** Public-key crypto uses user-specific keys that have a public component which, as long as they can be securely retrieved by any user (e.g., using a PKI system), significantly simply key management, as opposed to symmetric-key crypto where key management is really problematic, since we have to securely share (hard in practice) too many session-specific keys (inefficient in practice). This conceptual improvement comes at a cost though, because the new key structure (namely, the public key and the secret key of a user being correlated to "cancel" each other, yet the secret key remaining secret even when the public key becomes public), implementing public key crypto relies on algebraic mathematical structures that involves new computational assumptions (e.g., discrete logs or factoring) and heavier primitive operations (e.g., multiplications and exponentiations modulo large integer values), and thus results in less efficiency (2-3 order of magnitudes degradation in performance, e.g., from millions of operations to thousands of operations per second). Similarly, security often comes with some known weaknesses if quantum computing ever becomes practical (where, e.g., both discrete logs and factoring become easy to solve).
>
> - **Exemplary:** Essentially as above.
> - **Adequate:** Explanation is in the correct direction but too vague or less accurate.
> - **Poor:** Explanation is partially incorrect.

(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 $\sigma = \mathsf{Sign}(\mathsf{SK_S}, m)$...

C. If $(\mathsf{PK_S}, \mathsf{SK_S})$ is the public-key pair of S, m is sent signed with signature $\sigma = \mathsf{Sign}(\mathsf{PK_S}, m)$...

D. If $(\mathsf{PK_R}, \mathsf{SK_R})$ is the public-key pair of R, m is sent signed with signature $\sigma = \mathsf{Sign}(\mathsf{PK_R}, m)$...

(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 server 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**