Name

CWID

# Exam

# Monday, October 25th 2:00-3:30pm

# CS458 - Fall 2021 - Midterm

---

*Please leave this empty!*

1.1 | 1.2 | 1.3 | 1.4 | 1.5 | 1.6 | Sum

# Instructions

- **You have to hand in the assignment to the instructor**
- **This is an individual and not a group assignment. Fraud will result in 0 points**
- Things that you are **not** allowed to use
  - Personal notes
  - Textbook
  - Printed lecture notes
  - Phone
- You are allowed to bring one page (both two sides can be used) of cheat sheet that must be turned in with the exam
- The exam is **90** minutes long
- For your convenience the number of points for each part and questions are shown in parenthesis.

## Question 1.1 (66 Points)

1. (**3 pts.**) "CIA" stands for three important computer security goals. What are they?

   ----------, ----------, ----------

2. (**3 pts.**) Which of the following most accurately defines a *threat* (circle only one)

   - A means to prevent a vulnerability from being exploited
   - Weakness in the system that could be exploited to cause loss or harm
   - Set of circumstances that has the potential to cause loss or or harm
   - When an entity exploits a vulnerability in a system

3. (**3 pts.**) In World War II, Germans used machines called "Enigma" to encrypt their communications. The code was broken partly because the allies learned that one message always started with "nothing to report" and was sent daily using that day's rotor configuration. What type of attack best describes the following example? (circle only one)

   - Cipher text only
   - Known plain text
   - Chosen plain text

4. (**3 pts.**) Which of the following statement describes the advantage of AES over 3DES? (circle all that apply)

   - AES is faster.
   - AES has a larger key space to mitigates exhaustive search.
   - AES has a larger block size, and hence the same key can encrypt more messages before it is compromised.

5. (**3 pts.**) Alice and Bob are both using crypto to communicate with other people. Alice doesn't want Bob eavesdropping on her messages, and vice versa. They each need to choose algorithms and keys. Which of the following choices will protect one from eavesdropping by the other? (circle all that apply)

   (a) Use different algorithms and the same key.
   (b) Use the same algorithm and the same key.
   (c) Use the same algorithm and different keys.
   (d) Use different algorithms and different keys.

6. (**3 pts.**) Which of the following is an asymmetric key algorithm? (circle only one)

   (a) DES

   (b) AES

   (c) RSA

   (d) 3DES

7. (**4 pts.**) A birthday attack on a hash function $h$ is a way of finding inputs $x$ and $x'$ such that $x \neq x'$ but $h(x) = h(x')$. Circle each TRUE statement below. (circle all that apply)

   - For some hash functions, a birthday attack can be defeated by limiting the size of the hash input.
   - The amount of work involved in a birthday attack on a hash function increases as the square root of the size of the inputs to the hash function.
   - The amount of work involved in a birthday attack on a hash function increases as the square root of the size of all the possible outputs of the hash function.

8. (**3 pts.**) Bob sends Alice an encrypted message using AES. What key would Alice need to use to decrypt the message? (circle only one)

   (a) Bob's public key

   (b) Bob's private key

   (c) Alice's public key

   (d) The same key that Bob used to encrypt the message

9. (**3 pts.**) Alice transmits a message to Bob using a stream cipher. During transmission, an error causes a single bit in the ciphertext to change. How does this affect the decrypted message? (circle only one)

   (a) The decryption process corrects the error.

   (b) The decrypted message contains a 1-bit error in the same location.

   (c) The message is readable up to the bit containing the error and scrambled after that point.

   (d) The entire message is unreadable after it is decrypted.

10. (**4 pts.**) To create a key using the Diffie-Hellman algorithm, Alice uses numbers $\alpha$, $a$, and $\alpha^a \bmod p$, while Bob uses numbers $\alpha$, $b$, and $\alpha^b \bmod p$. The key they share is $\alpha^{ab} \bmod p$. In the set below, circle every number that is secret

$$\{\alpha, \quad \alpha^a \bmod p, \quad \alpha^b \bmod p, \quad a, \quad b, \quad \alpha^{ab} \bmod p\}$$

11. (**8 pts.**) We know that Alice can create an evil message $m$, factor it as $m = m_1 \times m_2$, and try to trick Bob into applying RSA signatures to $m_1$ and $m_2$, and then claim that Bob signed $m$ instead. Bob can deflect this attack by (circle all that apply)

    - insisting on signing hashes of $m_1$ and $m_2$ instead
    - sign $m_1$ and $m_2$ using different RSA key pairs
    - appending information on $m_1$ and $m_2$, such as "Bob signs this for Alice"
    - using a different key pair for signing than he does for encryption

12. (**4 pts.**) Order the following four items to match with the process of digital signature generation and verification: (circle one)

    1. Encrypt the digest with your private key.
    2. Compare the message digest to one you created.
    3. Generate a message digest.
    4. Decrypt the signature with the sender?s public key.

    (a) 4, 2, 1, 3
    (b) 3, 4, 2, 1
    (c) 1, 4, 3, 2
    (d) 3, 1, 4, 2

13. (**3 pts.**) What is TRUE of a *nonce* (circle all that apply)

    - It is secret.
    - It is included in a key exchange algorithm to defend against replay attacks.
    - It must be randomly generated by a cryptographically secure random number generator.
    - It must contain enough bits to be distinguishable from all other nonces recently used.

14. (**4 pts.**) Recognize the following modes of encryption for block ciphers based on their mathematical expressions. Notation: $P_i$ is the $i^{th}$ block of plaintext, $C_i$ of ciphertext, $E_k()$ is the block cipher encryption function, and $\oplus$ denotes the XOR function. for example: $C_i = E_k(P_i)$, uses ECB mode.

    - $C_i = E_k(C_{i-1} \oplus P_i)$ Answer:
    - $C_i = E_k(i) \oplus P_i$ Answer:

15. (**5 pts.**) Suppose you know that cipher-text **D T Z B N Q Q S J A J W B F Q P F Q T S J** has been encrypted using a Shift cipher. The key of that cipher is (circle only one)

    - 3
    - 4
    - 5
    - none of the above

16. (**10 pts.**) Let the two primes `p = 5` and `q = 11` be given as set-up parameters for RSA.

    - Encrypt the message `m = 10`. Show your work for full credit.

Scratch Page - This page is intentionally left blank