Midterm Exam (Mock)

This is a closed-book test. You may not refer to any books or notes during this examination, and you may not use any electronic aid.

Write your answers legibly. The intended answers fit within the spaces provided on the question sheets. You may use the back of the preceding page for scratch work. If you run out of room for an answer, continue on the back of the page and clearly mark your answer.

This is a mock exam (with 3 questions) designed for around 30 mins. The original midterm exam will have 5 (similar) questions in total and the duration will be 60 mins.

Time limit: **30 minutes**.

Write and sign the honor code pledge:

> "*I have neither given nor received unauthorized aid on this examination, nor have I concealed any violations of the Honor Code.*"

_____

_____

_____

_____

(Signature)

_____

(Print your name)

_____

(UA NetID)

1. Short Answer

(a) [2 points] How does the Linux kernel expose cryptographically secure random data? Where does the data come from (what provides the entropy)?

(b) [2 points] What is a one-time pad? Why is reusing a pad insecure?

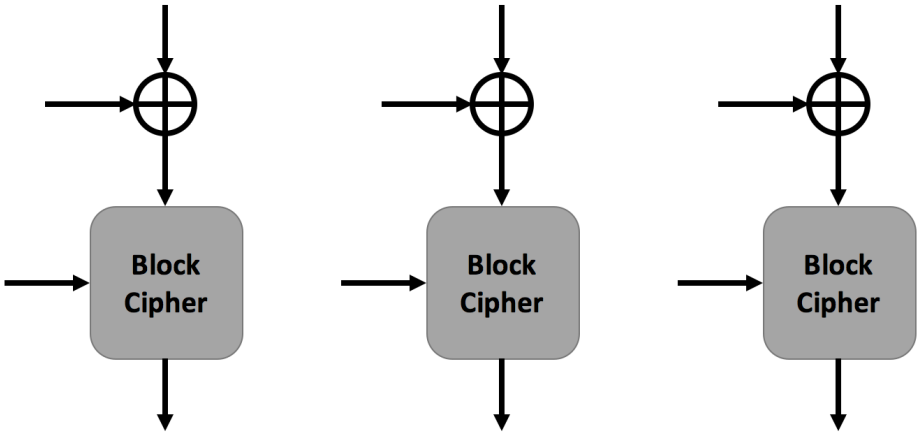
(c) [2 points] What security guarantee does HMAC provide? Can HMAC be used for digital signatures? If yes, how? If no, why not?

(d) [2 points] Why padding oracle is different than the decryption oracle?

(e) [2 points] What are the differences between role-based and attribute-based access control?

2. Ciphers

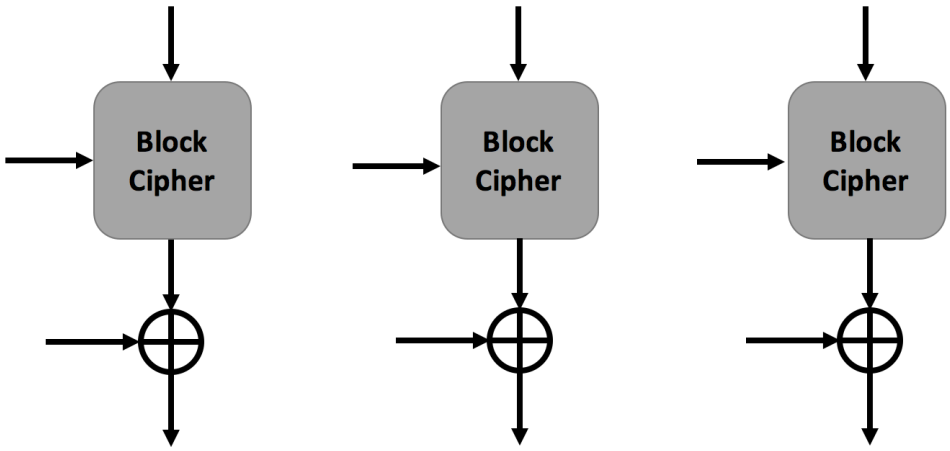
(a) [3 points] Show how to connect the three Block Cipher blocks below to perform **encryption** in Cipher Block Chaining (CBC) mode. In addition to connecting the blocks, label the plaintext **P1**, **P2**, and **P3**; the ciphertext **C1**, **C2**, and **C3**; the key **K**; and the Initialization Vector **I.V.**.



(b) [2 points] If the block cipher used is AES256 and the plaintext is 1024 bits how much padding is required? Remember that the block size of AES256 is 128-bits even though the key is 256-bits.

(c) [2 points] How do you select an value for I.V.?

(d) [3 points] Show how to connect the three Block Cipher blocks below to perform **decryption** in Cipher Block Chaining (CBC) mode. In addition to connecting the blocks, label the plaintext **P1**, **P2**, and **P3**; the ciphertext **C1**, **C2**, and **C3**; the key **K**; and the Initialization Vector **I.V.**.



3. Public Key Crypto

Professor Vuln's lab needs help in designing a security protocol so that the members of the lab can securely communicate. However, they are having trouble remembering their security principles and crypto primitives, and need your help to design the system.

The members of the lab have already decided that they will incur the cost of using a *public key infrastructure*. For a particular user *user*, denote their public key as Pub_{user} and their private key as $Priv_{user}$.

(a) [4 points] Define *message integrity*, and give an example of how we ensure it in modern systems.

(b) [3 points] Design a simple protocol that uses some (or all!) of the above keys that ensures that the system has integrity, but not confidentiality.

(c) [3 points] Design a simple protocol that uses some (or all!) of the above keys and ensures that the system has confidentiality, but not integrity.