CS 199 COMPUTER SECURITY FALL 2022 MIDTERM I

Instructor Calvin Deutschbein

Roster Name	
Sign here to affirm the Honor Code	

This exam will be timed to take 60 Minutes.

It will be scored out of 200 Points.

It will make up 20% of Final Grade.

SECTION I: CRYPTOLOGY 60 Points

Part 1: Terminology: 4 Questions @ 5 Points each = 20 Points

Which of the following best describes the technology implemented by symmetric-key algorithms?

A. Blockchain public ledger
B. Block cypher compression function
C. Inverse functions
D. Public key encryption

Which of the following best describes the technology implemented by Bitcoin?

A. Blockchain public ledger
B. Block cypher compression function
C. Inverse functions
D. Public key encryption

Which of the following best describes the technology implemented by RSA?

A. Blockchain public ledger
B. Block cypher compression function
C. Inverse functions
D. Public key encryption

Which of the following best describes the technology implemented by SHA-256?

A. Blockchain public ledger
B. Block cypher compression function
C. Inverse functions
D. Public key encryption

Part 2: Short Response: 2 Questions @ 10 Points each = 20 Points

Briefly describe one of the following technologies:

- Blockchain
- Symmetric-key algorithms

Describe in your own words the distinction between compression encryption and public key encryption.

Part 3: Written Response: *20 Points*

Write two Python functions, “hash” and “unhash”, that both accept as input a single integer and produce as output a single integer such that:

- hash(x) != x
- unhash(hash(x)) == x

SECTION II: THREAT 90 Points

Part 4: Bits and Bytes: 4 Questions @ 5 Points each = 20 Points

Recall that **bitwise operations** generalize **logical operations** like ‘not’, ‘and’, ‘or’, and ‘xor’ (exclusive or). For the following, compute the bitwise result over the binary values.

What is the value resulting from the following **bitwise not**: ~0b10?

A. 0b00
B. 0b01
C. 0b10
D. 0b11

What is the value resulting from the following **bitwise and**: 0b1100 & 0b1010?

A. 0b1000
B. 0b1110
C. 0b0110
D. 0b0001

What is the value resulting from the following **bitwise or**: 0b1100 | 0b1010?

A. 0b1000
B. 0b1110
C. 0b0110
D. 0b0001

What is the value resulting from the following **bitwise and**: 0b1100 ^ 0b1010?

A. 0b1000
B. 0b1110
C. 0b0110
D. 0b0001

Part 5: Short Response: 2 Questions @ 20 Points each = 40 Points

Briefly describe how **bitwise operations** can be incorporated into hashing algorithms, such as SHA-256.

Unlike arithmetic operations, bitwise operations are not commonly used outside of the field of computing. Argue for the comparative merits and costs of using **bitwise operations** specifically for cybersecurity.

Part 6: Threat Modelling Exercise *30 Points*

Recall that threat modeling for some system, including computer systems, proceeds in four steps:

- Diagram. What are we building?
- Identify threats. What could go wrong?
- Mitigate. What are we doing to defend against threats?
- Validate. Have we acted on each of the previous steps?

Consider the development of a computer system to provide assistance to undocumented workers facing workplace discrimination over the Internet by providing connections to frontline support workers or access to electronic funds. Provide a threat model for this system.

SECTION III: THEORY 50 Points

Part 7: Short Response: 2 Questions @ 25 Points each = 50 Points

Blockchains often use compression functions in their implementations. However, they are not the only application for compression functions. Describe one example of how a compression function can provide a valuable service to users other than blockchain.

Public key encryption is often used to transmit information securely over public networks, but is not the only technique we have shown for encrypting information. Describe the benefits and limitations of public key encryption compared to other techniques.