CS 370 Introduction to Security **Week 3: Problem Set 3**
Instructor Name: Rakesh Bobba

Introduction

The purpose of this assignment is to help you gain a better understanding and insight into the cryptographic concepts and primitives we learned about in Week 3 and help you learn how they are applied.

Before beginning make sure you have watched the lecture videos on the following and completed the associated practice quizzes.

- Cryptographic Hash Functions
- Message Authentication Codes
- Intro to Public-Key Crypto
- Diffie-Hellman Key Exchange
- RSA
- Digital Signatures

Also make sure you have read this week's assigned reading from the textbook.

Questions

Please answer all of the questions below.

Cryptographic Hashes & Message Authentication Codes (MACs)

Q1[3 pts]: What are the three key properties of a cryptographic hash?

- Pre-image Resistance
- Weak-Collision Resistance
- Strong Collision Resistance

Q2 [3pts]: What is a birthday attack? Consider a hash function that maps inputs to a 32-bit hash. If an attacker launches a birthday attack, approximately how many steps will it take the attacker to find a collision with a 50% probability of success?

- A birthday attack is where the attacker generates $2^{m/2}$ variations of a valid message with the same basic meaning, as well as $2^{m/2}$ variations of a fraudulent message and finds a pair of valid and fraudulent messages that have the same hash value. Then, when the valid message is signed by the user, the valid message is replaced with the fraudulent message.
- The number of steps to have a 50% probability of success is $2^{32/2}$.

Q3 [4 pts]: What is the difference between a cryptographic checksum and a message authentication code? What primitive should one use to integrity protect files being transferred on an open channel?

- A MAC is proof of a message's integrity and provides authentication, whereas a checksum just guarantees the message's integrity.

- To integrity protect files that are being transferred on an open channel, a checksum should be used.

Public-Key Cryptography (Diffie-Hellman, RSA, Digital Signatures)

Q4 [3 pts]: Name three differences between secret-key cryptographic schemes and public-key cryptographic schemes?

- Decryption Speed
- Secret-key involves keeping the key secret (as the name implies) whereas public-key allows one key to be public.
- Public-key systems are based on solving hard problems, such as factoring large numbers.

Q5 [3 pts]: What is a digital signature? What security properties does it provide?

- A way to verify the authenticity of a message.
- Provides Confidentiality, Integrity, and authentication.

Q6 [3pts]: How are digital signatures different from MACs? Contrast the security properties they provide.

- MACs provide Authentication and Integrity.
- Digital signatures provide Authentication, Integrity, and Non-repudiation.
- MACs do not provide non-repudiation because it is possible for an entire network to share one secret key.

Q7 [9pts]: Alice owns a public-private key pair (PKA, SKA); Bob owns a public-private key pair (PKB, SKB); Assume that they know each other's public keys and answer the following questions:

If Alice wants to send a secret message M to Bob, what should she do? Show what needs to be transmitted using the notation used in class.

- $M^e \bmod n$

Bob receives a 128-bit AES key and the message "from Alice: use this key to send me your credit card number", both enciphered with his public key. Should Bob do what the message says? Assume Bob does want to send Alice his credit card number. If yes, why? If not, how should the message have been enciphered?

- Bob should not send his credit card number, chiefly because that's a bad idea anyway, but also because the message was encrypted the wrong way.
- The way that the message should have been encrypted is to have the message encrypted with Bob's public key and its hash encrypted with Alice's private key. This way, the hash only decrypts with her public key, and that is how Bob would verify that Alice is the one who actually sent the message.
- Bob would verify that Alice was the sender by first computing the hash of the message he received, next, he would use Alice's public key to extract the hash that he received and compare it to the one he computed himself. Finally, if they matched, then Alice was the sender.

If M is a really long message, how should Alice transmit the message while keeping it secret and minimizing the effort? Please explain.

- Compute a hash of the message and sign it using her private key. Transmit this, along with the message, to the recipient. The recipient then decrypts the signature and checks the value of the hash against their own computed hash of the message.

Q8 [3 pts]: Do digital signatures and MACs increase the length of message to be transmitted? Explain Why?

- Digital signatures and MACs do increase the length of a message to be transmitted because digital signatures append an encrypted version of a message to the end of the original message and MACs are transmitted along with the message to the receiver.

Q9 [3 pts]: Using the notation from the class, show how a message m is signed with an RSA key-pair (N, d, e).

- $(m^e)^d = m \pmod N$

Q10 [4pts]: Contrast man-in-the-middle and meet-in-the-middle attacks.

- A Man-In-The-Middle attack is an adversary intercepting a conversation between two entities, while a Meet-In-The-Middle attack is breaking encryption by trying to brute force it from both ends; I.e. brute forcing encryption and decryption to find a matching value that “meets in the middle.”

Q11 [3pts]: Is it important to hash the message for digital signatures?

- No. Hashing the entire message is computationally expensive, especially with a large message. It is better to hash the signature.

Q12 [3 pts]: Does the hash function used in an RSA signature need to be a keyed hash function? Why or why not?

- Yes, because using a private key to hash a signature gives the receiver of the message a way to verify who the sender was.

Submission Details

Submit a PDF file with the questions and your corresponding answers.
The assignment is worth 44 points. It is due Wednesday of Week 4 at Midnight.