**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?

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?

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?

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

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

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

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

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 notaion used in class.

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?

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

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

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

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

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

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

# 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.