**Hsiang Lo**

**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?

* + **Efficient:** For any x in A, h(x) is easy to compute
  + **Pre-image Resistance**: For any y in B, it is computationally infeasible to find x is a subset of A such that h(x) = y
    - E.g, computing x ^ 3 is easy by hand but computing cube root of x is hard.
  + **Weak-Collision Resistance**: Given any x in A, it is difficult to find another element of that set such that the hash value matches even though they are different.
  + **Strong-Collision Resistance**: It is computationally infeasible to find two inputs x, x’ in A such that x != x’ and h(x) = h(x’)

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 reflects back to the idea of paradox. It works thus by having the opponent generates a 2^(m/2) variations of a valid message all with essentially the same meaning. Opponent also generates a 2^(m/2) variations of a desired fraudulent message. The attacker will then have two sets of messages compared to find pair with same hash. This would result in the probability of > 0.5, or 50% of finding a collision. After this, the attacker can give a valid message to be signed only to later substitute the valid message with fraudulent message which will have a valid signature. Given the input is 32 bits, it would require 2^16 bits of steps to find a collision with 50% probability.

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 cryptographic checksum is an unencrypted one-way hash functions with no secret key that’s easy to compute one direction but not the other. A message Authentication Code or MAC is used to when the hash has to be pass along with the message. Message Authentication Code should be used when the hash has to be pass along with the message in order for the hash to be accessed and protected by a key. This is more useful for open channels. They both guarantees integrity, but MAC guarantees both integrity and authentication since the MAC cannot be modified without the knowledge of the key.

In this case, because it’s an open channel, Mac 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?

Public key crypto uses private/public key pair. Depending on the usage, it’s typically used for encryption/decryption and signing/verification. Of all the differences, these three are the most prominent differences between public-key schemes and private-key schemes. First, private-key are faster than public-key. Private key is symmetrical, public key are asymmetrical. Private (symmetric) key is truly private. It’s only available with only the two communicating parties while public keys can be made public. Public key is used mainly for encryption, private key is used for decryption. A

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

**Digital Signature** uses a private key to encrypt a hash value (message digest). The act of encrypting this hash value with a private key is called digitally signing a message. A digital signature attached to a message proves the message originated from a specific source and that the message itself was not changed while in transit. It provides authenticity, non-repudiation and integrity. It basically checks for the user to see if it came from where it says it did, if the message was changed and also to trace back to where it’s from.

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

In both Mac and digital signature schemes, you have two algorithms.

* Generation – Given the message m and a key K1, compute the MAC value or signature s.
* Verification – Given the message m1 a key k2 and the MAC value or signature s, verify that they corresponds to each other (MAC:s value or signature is valid for the message m, using verification key k2)
* Mac mainly focuses on integrity and authenticity
* Digital Signature focuses on integrity, authenticity and non-repudiation

With a MAC, keys K1 and k2 are identical, with a signature, the verification key2.is mathematically linked with k1 but not identical and it is unfeasible to recompute k1 from k2 or to generate a valid signature when you only know k2.

Thus, signature dissociate the generation and verification powers. With a MAC, anyone who know the MAC can generate MAC value on their own. With signature, the key can be made public with the generation key private. Signatures are for when you want to produce a proof verifiable by third party.

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.

Given that both Alice and Bob own a public-private key pair, and given that they both know each other’s public key up front, this eliminated the need to use Diffie-Hellman key establishment to share key without being compromised (As it has already been done).

Alice would need to encipher the message with Bob’s public key, PKB, so that then Bob can use his private key SKB to decrypt the message.

Notation used in class

Alice -> M(PKB) -> Bob

Or

M = D(E(m,PKB),SK)

Where M is the original message,

PKB is Bob’s public key,

E is the encryption algorithm,

C is the cipher text,

D is the decryption algorithm.

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?

No he should not since the message was enciphered using Bob’s public key. Anyone with access to Bob’s public key can send the said message, claiming to be Alice.

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

This is when you combine symmetrical and unsymmetrical methods. Using a randomly generated symmetric key for most of the message. Then you can use the public key to transmit. With the last blocks for integrity.

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

Yes because besides the message that is being transmitted, there is paddling involved and the digital signature or MAC is randomly generated andw ill add to the length of the message.

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

Using the notation from the class to show how a message m is signed with an RSA key-pair, it can be signed as follows, M = m ^ d mod N

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

Man-in-the-middle is when there is an attack between decipher and encryption that pretends to be the trusted party while meet-in-the-middle refers to brute force using both encryption side data and decrypted side data.

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

Yes, it is important to hash the message for digital signature prevents someone from accessing the signature without the key and reduces the computational effort since hashing output is less expensive.

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 the hash is keyed using the signer’s private key, which produces the signature that is attached along with the certification.

During verification, the digitally signed data ‘s signature is decrypted using singer’s public key. The hash from that is checked with data’s hash after hash function. Only if it’s equal do the decryption/encryption work for RSA.

# 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.