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?

- One Way: i.e. not reversible (with current computational capabilities)
- Efficient: i.e. easy to compute the hash of something.
- Collision Resistant: incorporates strong and weak collision resistance. This means that it is unlikely that disparate input values will collide to the same hash output.

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 stems from the birthday paradox that [briefly put] states it is far more likely that there are two people in a room of n that have the same birthday, then that there is someone in that room with the same birthday as you. This applies to hash collision resistance, because with strong collision, we are trying to find two values with the same hash output – i.e. two identical 'birthdays'. The takeaway of the birthday paradox is that there is a 50% chance of collision when you have examined sqrt(<hash_output_space>). Therefore, once you have completed searching sqrt(<hash_output_space>) you have a 50% chance of finding a collision. sqrt(<hash_output_space>) for an x bit hash output corresponds with $2^{x/2}$ hashes. For

200-bit hash output, the attacker only needs to compute 2^{100} hashes to have a 50% chance of finding a collision.

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 checksum (aka hash) is a tool that can generates an output set of bits based on an input set (and is one way, collision resistant…). This differs from a MAC as a MAC combines hashes and the message itself to guarentee integrity, where a hash could be recalculated for a message modified in transit.
- I would use an HMAC primitive.

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 schemes are slowere (sometimes up to 10,000 times slower than private key schemes).
- Private Key cryptography schemes use a shared private key that is only known to the two parties sharing data, whereas asymmetric crypto schemes use a shared public key (known to all) and each user has their own disparate private key.
- Private key schemes are quite a bit older than asymmetric, public key schemes.

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

- A digital signature is a cryptographic method of checking the authenticity of something sent between people (public or private channel).
- This provides Integrity, Accountability, Authenticity

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

- Because MACs are composed using a symmetric (private) key, the result is that when contrasted with Digital Signatures, they lack non-repudiation (aka authenticity). This is because Digital signatures use Asymmetric crypto, that provides non-repudiation.
- They still both retain the ability to protect Integrity and Authenticity.

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.

- Alice needs to send c = E(m, PKB). This will make it so that only D(c, SKB) will result in the message being decoded, something only Bob can do.

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?

- It would appear that Alice is trying to get Bob to use a symmetric key to send his credit card data (I’ll also assume Alice and Bob know each other, otherwise the transfer of credit card data is not recommended). Therefore, he can do as Alice says – use the AES key to encrypt and send his credit card number to her. Despite that, I would advise Bob to encrypt the Credit Card data with the AES-128 key, then encrypt it again with Alice’s PKA key, and send that to her (yes, that is redundant…). Otherwise, Bob could assess that he should just send it using Alice’s PKA as that is how she sent him the AES key, so the AES key’s security is only as good as that of the symmetric key protocol, and the security of Alice’s machine, where both of these keys are stored. Therefore, for redundancy, I would tell Bob to do both AES and asymmetric encryption with PKA, but if he were to object, I would recommend he uses asymmetric encryption with PKA.

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

- Alice should use hybrid encryption – what she would do is use a block cipher to encrypt the message using a symmetric key of a ‘safe’ algorithm. Then she should send an RSA (or other asymmetricly encrypted) message containing the symmetric key, encrypted with the recipient’s PK. Lastly, she should send the ciphertext produced with the block cipher.

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

- These do increase the length of the message (or of the total data sent) as the encrypted hash **and** the message are sent.

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

- Signature = F(h(M), e)
- Signature can be sent independently or appended to message.

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

- For the Man in the middle, an attacker must intercept all the communications from the start (public key exchange) between two users. This allows each user to think they are messaging the other, while they are both messaging through the ‘middle’ user.
- A Meet in the Middle attack is an attack where multiple iterations of the same encryption operations can ‘cancel out’ and instead of adding the number of attempts need

(key_length_1 + key_length_2), they do not significantly increase the complexity needed for an attacker to compromise the security through brute force.

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

- Yes it is. If the message were nor hashed before being encrypted, then the encryption algorithm might have to do much more work (or not be able to handle the message) because of its size. When you hash something, you get a hash that is of a fixed, low, length that can then be encrypted.

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

- It should not need to be keyed, as it is encrypted with RSA after the hash is generated, so there is already a keyed operation going on there, and compromise of that key could mean that keying the hash would be useless.

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.