Practice Questions for Computer Security

CS370/ECE499

Hash Functions and MACs

1. What are the three key properties of a cyrptohraphic hash?
   [Bonus] Which of the three properties implies the others. Please explain.

2. 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?

3. 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 and Digital Signatures

1. Name three differences between secret-key cryptographic schemes and public-key cryptographic schemes?

2. Alice owns a public-private key pair (PK_A, SK_A); Bob owns a public-private key pair (PK_B, SK_B); Assume that they know each other's public keys and answer the following questions:

   a. 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.

   b. 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?

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

3. How are digital signatures different from MACs?

4. Contrast man-in-the-middle and meet-in-the-middle attacks.

5. Is it important to hash the message for digital signatures?

6. When a hash function is used in the generation of digital signatures, what property(ies) of hash function is critical for the security of such signatures?

7. When using HMAC with a key size of K bits and output of L bits what is i) the security strength against forgery, and ii) security strength of the HMAC algorithm?
   [Hint: See NIST SP 800-107 -- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf]