# CSE543/Fall 2007 - Cryptography Mini-Exam

**Tuesday, September 25, 2007 — Professor Trent Jaeger**

Please read the instructions and questions carefully. You will be graded for clarity and correctness. You have 45 minutes to complete this exam, so focus on those questions whose subject matter you know well. Students who try to read the papers in order to find an answer will not likely do well. Write legibly and check your answers before handing it in.

**Short Answer - some will be one or two words – no more than 3 sentences**

1. (*3pts*) When a cryptographic construction provides message *authenticity*, what does the receiver learn?

   *answer*: Authenticity enables the receiver to verify the identity of the sender of the message, implying the message's integrity.

2. (*3pts*) What is the probability of finding a *collision* for an ideal 60-bit hash function? What is the main reason for this probability?

   *answer*: 1 in $2^{30}$. Due to the *birthday paradox*.

3. (*3pts*) Define the two properties of true cryptographic hash functions.

   *answer*: *One-way property* states that it is computationally intractable to compute the pre-image of a digest $h^{-1}(y) = d$. The *collision-free property* states that it is computationally intractable to find two inputs whose hash values are the same.

4. (*3pts*) What is the main purpose of the last two messages in the Needham-Schroeder symmetric key protocol?

   *answer*: B wants to prove that A really has possession of the session key provided in the ticket in the third message. B provides a nonce to A that must it must decrypt and modify to prove its ability to use the session key.

5. (*3pts*) Specify the trust model of a PKI system? That is, what is the CA trusted to state?

   *answer*: CA is trusted to verify the mapping between public keys and identities. CA is trusted to protect its private key from being leaked. The user must trust her machine to protect the generation and use of her private key.

6. (*3pts*) How does a private key signature ensure *non-repudiability*?

   *answer*: Private key can only belong to signer, and signing the hash ensures that the message's integrity can be associated with the private key encryption.

**Long Answer - no more than 2 paragraphs**

7. (*7pts*) Why should you include a *message authentication code* (MAC) with a message? What is the difference between a MAC and an HMAC?

   *answer*: Provide authenticity and especially integrity. HMAC is a special form of a MAC $HMAC(k, d) = H(K + H(k + d))$ that prevents extension attacks.

8. (*7pts*) What purpose does the *authenticator* in a Kerberos message serve? Detail one flaw Merritt and Bellovin identified in its design.

   *answer*: It is used to provide fresh proof that the principal really knows the session key. The authenticator includes timestamp and identity of the sender encrypted with the associated ticket's session key to justify the source and the message freshness. The timestamp is valid for 5 minutes, so someone can replay in this window.

**Word Problems - take your time and answer clearly and completely.**

9. (*10pts*) Suppose Alice wants to send a message to Bob containing her name $N$, her computer's IP address $IP$, and a request $R$ for Bob. Design the cryptographic messages that Alice must send to meet the security requirements below. Assume that Alice and Bob share a symmetric key $K$ and have securely distributed their public keys $K_A^+$ and $K_B^+$.

   Assume that all the messages include Alice's name, IP address, and the request.

   (a) (2pts) Using the symmetric key, design a message that enables Bob to verify that the message's integrity has not been violated and that it is from Alice.

   (b) (2pts) Using the symmetric key, design a message that protects the confidentiality of the request only and ensures that Bob can verify the message's integrity and source.

   (c) (2pts) Using public key cryptography, design a message that enables Bob to verify that the message's integrity has not been violated and that it is from Alice.

   (d) (2pts) Using public key cryptography, design a message that protects the confidentiality of the request only and ensures that Bob can verify the message's integrity and source.

(e) (2pts) What is the major advantage of public key cryptography over symmetric key cryptography?

*answer*:

Suppose the message is $C = \{N, IP, R\}$.

(a) $C + HMAC(K, C)$
(b) $N + IP + E(K, R) + HMAC(K, C)$
(c) Where $S(K_A^-, C)$ is signature, message is: $C + S(K_A^-, C)$
(d) $N + IP + E(K_B^+, R) + S(K^-, C)$
(e) in public key secure key distribution is easier – everyone can know it

10. (*10pts*) Suppose Alice wants to send her Bank a message that includes her promise to pay Charlie \$50 dollars. Alice and the Bank have a shared secret $X$. Alice initiates a conversation with the Bank by sending: $A + B + n$ (Alice's identity, the Bank's identity, and a nonce). Assume that Bank tracks the nonces used by Alice for $X$.

    Answer the following questions.

    (a) (3pts) Specify a valid reply for the Bank (i.e., a message generated by the Bank to be sent to Alice) that would enable Alice to verify that the reply came from someone who knows the secret $X$.

    (b) (2pts) In order to setup a secure communication, Alice and the Bank need a secret session key. Suppose that the Bank chooses a session key $K$ by XORing some pseudorandom data with $X$ and includes it with the reply in (a) above. Extend message (a) to provide the session key to Alice securely as well.

    (c) (3pts) Now, Alice can submit her message ("Pay Charlie \$50 from my account") to the Bank. Write the message in such a way that Charlie cannot replay it (*Hint: you will need to add something to the message that the Bank is capable of checking to prevent replay.*).

    (d) (2pts) Why is it that a "man-in-the-middle" attack cannot result in an adversary determining the key $K$ in this protocol?

    *answer*:

    Lots of answers are possible for this. This is what I would do.

    (a) $A + B + n + HMAC(X, A + B + n)$ – must be different than the message Alice sent using X
    (b) $A + B + n + E(X, K) + HMAC(X, A + B + n + K)$

(c) Call $M$ the message and include $c$ a counter for the messages in the session. Then $A + E(K, M + c) + HMAC(K, A + M + c)$ protects M's secrecy, ensures that Charlie cannot replay, and protects the integrity of the message.

(d) The key $K$ is derived from the secret $X$ that only the Bank and Alice have access to. The adversary cannot establish an old session because the nonce cannot be replayed (Bank maintains set for $X$ by assumption). Also, A, B are included in the messages to ensure that no man-in-the-middle is replaying authentication messages.

11. (*10pts*) Answer the questions below regarding key generation with Diffie-Hellman and RSA.

(a) (2pts) Suppose the Diffie-Hellman public values $p$ and $g$ are 7 and 4, respectively. Compute a legal $y$ value.

(b) (2pts) Suppose your partner's $y$ value is 3. What is your shared key?

(c) (2pts) Suppose that you are computing an RSA key pair. What are $p$ and $q$ and $\phi(n)$ for an $n = 51$?

(d) (2pts) Find a legal RSA public key pair for this $p$ and $q$.

(e) (2pts) How many possible values for $e$ are there?

*answer*:

(a) $y = g^x mod p$ where $x$ could be pretty much any value, I will choose 4. Therefore, $y = 4^4 mod 7 = 256 mod 7 = 4$.

(b) The shared key $z = y^x mod p = 3^4 mod 7 = mod 7 = 4$.

(c) $p = 3$, $q = 17$ (or vice versa), and $\phi(n) = 2 * 16 = 32$.

(d) A valid $e$ is 5, as it is relatively prime to 32. Given $e = 5$, $demod\phi(n) = 1$, so $d$ can equal 13 ($5 * 13 mod 32 = 1$). Officially, $d = (13, 51)$ and $e = (5, 51)$.

(e) Odd numbers less than 32 = 16. Other odds are permissible in general too.