CS 329E Quiz 4: April 24, 2014

Name: __________________________________________

Notice that this quiz has two sides.

1. (5 points) For each of the following, fill in the word or phrase that best matches the description provided.

   (a) ______________________ General term for a participant in a protocol.

   (b) ______________________ International standard for certificates.

   (c) ______________________ A certificate vouches for the correspondence between identity and _____.

   (d) ______________________ Property that holds when a party can’t claim not to have sent a message.

   (e) ______________________ A covert channel using the duration of events in the system is called a _____.

2. (5 points) PGP allows the user to send messages in various formats to accomplish specific security goals. From an abstract perspective, the three formats discussed in the lectures are:

   1. $S \to R : \{K\}_{K_R}, \{M\}_{K}$
   2. $S \to R : \{h(M)\}_{K_s^{-1}}, M$
   3. combination of the two above.

Write 1, 2, or 3 to indicate which of these provides the security service? Choose the minimal answer—i.e., if 1 or 2 suffices, don’t choose 3. Note: encryption alone does not guarantee message integrity.

   (a) _____ Message integrity   (b) _____ Nonrepudiation
   (c) _____ Confidentiality     (d) _____ Authentication
   (e) _____ Combination of a, b, c and d

Page total: _____
3. _____ (2 points) Which of the following is not typically a property of a digital signature?

   A. authenticates the signer
   B. unforgeable
   C. tamperproof
   D. confidential
   E. not reusable
   F. All of the above are properties of digital signatures.

4. _____ (2 points) Which of the following is a true statement?

   A. ECB xors each successive plaintext block with the preceding ciphertext block prior to encryption.
   B. Using an encryption algorithm in a key stream generation mode can be used to generate a pseudorandom bit stream.
   C. Using a one-time pad with a pseudorandom bit stream yields a perfect cipher.
   D. Encryption with an RSA private key is a privacy transformation, not an authenticity transformation.
   E. None of the above are true.

5. (6 points) The slides presented an abstract version of a certificate with the following form:

   \[(Y, K_Y, \{h(\{Y, K_Y\})\}_{K_X^{-1}})\]

   Answer the following questions (briefly):

   A. What is Y? 
   B. What is \( K_Y \)?
   C. What is \( h \)?
   D. What is \( K_X^{-1} \)?
   E. Whose certificate is this?
   F. Who is the certifying authority?