CECS 378 Assignment 2 - Cryptography

20 points

Assignment Description. Answer the following questions from the Chapter 2, 20, and 21 readings from your textbook. Be through and complete with your answers. You *may* work on these questions with a partner (no more than two working together), but **both** students must submit the document individually on Beachboard Dropbox along with both of your names on each submission.

1. How many keys are required for two people to communicate via a symmetric cipher?
2. What is a message authentication code?
3. What are the principal ingredients of a public-key cryptosystem?
4. With the ECB mode, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates. For example, an error in the transmitted C_1 (Figure 20.6, pg. 622 in CSPaP) obviously corrupts P_1 and P_2.
   (a) Are any blocks beyond P_2 affected?
   (b) Suppose that there is a bit error in the source version of P_1. Through how many ciphertext blocks is this error propagated? What is the effect at the receiver?
5. You want to build a hardware device to do block encryption in the cipher block chaining (CBC) mode using an algorithm stronger than DES. 3DES is a good candidate. Figure 20.11 on pg. 632 in CSPaP shows two possibilities, both of which follow from the definition of CBC. Which of the two would you choose:
   (a) For security?
   (b) For performance?
   (c) And answer why for each.
6. Fill in the remainder of this table:

Mode	**Encrypt**	**Decrypt**
ECB	$c_j = E(K, P_j) \quad j = 1, ..., N$	$P_j = D(K, C_j) \quad j = 1, ..., N$
CBC	$C_1 = E(K[P_1 \oplus IV])$ $C_j = E(K, [P_j + C_{j-1}) \quad j = 2, ..., N$	$P_1 = D(K, C_1) \oplus IV$ $P_j = D(K, C_j) \oplus C_{j-1} \quad j = 2, ..., N$
CFB		
CTR		

7. Padding may not always be appropriate. For example, one might wish to store the encrypted data in the same memory buffer that originally contained the plaintext. In that case, the ciphertext must be the same length as the original plaintext. A mode for that purpose is the ciphertext stealing (CTS) mode. Figure 20.12a on pg. 633 in CSPaP shows an implementation of this mode.

   (a) Explain how it works.

   (b) Describe how to decrypt C_{n-1} and C_n.

8. It is possible to use a hash function to construct a block cipher with a structure similar to DES. Because a hash function is one way and a block cipher must be reversible (to decrypt), how is it possible?

9. Perform encryption and decryption using the RSA algorithm for the following:

   (a) $p = 3$; $q = 11$, $e = 7$, $M = 5$

   (b) $p = 5$; $q = 11$, $e = 3$, $M = 9$

   (c) $p = 7$; $q = 11$, $e = 17$, $M = 8$

   (d) $p = 11$; $q = 13$, $e = 11$, $M = 7$

   (e) $p = 17$; $q = 31$, $e = 7$, $M = 2$

10. Suppose we have a set of blocks encoded with the RSA algorithm and we do not have the private key. Assume $n = pq, e$ is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us in any way?

Deliverables. Submit the answers to the questions on **Beachboard Dropbox** by the indicated due date and time. Acceptable file submission formats are: .txt, .rtf, .odt, .doc, .docx, or .pdf.