Sujun Kim

Cecs 378

Assignment 2

1.How many keys are required for two people to communicate via a symmetric cipher?

- Since symmetric cipher requires same key, one is required for two people to communicate

2. What is a message authentication code?

- It is one-way hash function

3. What are the principal ingredients of a public-key cryptosystem?

- One private key and one public.

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 C1 (Figure 20.6, pg. 622 in CSPaP) obviously corrupts P1 and P2.

(a) Are any blocks beyond P2 affected?

- No

(b) Suppose that there is a bit error in the source version of P1. 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? I would choose round n for better security

(b) For performance? I would choose round 1 for easier analyzation

6. 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.

- First, the message to be encrypted would go through C1 and followed by CN-2 which would result an item to be used on next block CN

(b) Describe how to decrypt Cn−1 and Cn.

7. 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?

- Because hash function in this situation would be used to cipher encryption

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

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

- n = 33 o(n) = 20; gcd (o(n),e) = 1; 1 <e< o(n)

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

N = 55

O(n) = 4 *10 = 40

E = 3 gcd(on,e)= 1

3 gcdo(n),3) = 1

(b) p = 7; q = 11, e = 17, M = 8
n = 77
on = 7-1 * 11-1 = 6 *10 = o(N)17

(c) p = 11; q = 13, e = 11, M = 7
n = 143
on = 10 &12 = 120 on 11

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

9. 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?

- n = pq
- since e is public key plaintext block mustiby common factor of n meaning n^a
-