

Assignment #3

Due: Thursday, October 7, 2004.

Problem 1 (10 pts) Identify parts in the DES and the AES where (i) substitution cipher techniques are used, (ii) transposition cipher techniques are used, and (iii) techniques from the one-time pad cipher are used.

Even though techniques from substitution and transposition ciphers are used in DES and AES, explain why the parts using them are not substitution or transposition ciphers. Explain why the parts in DES/AES using techniques from the one-time pad cipher are not one-time pad ciphers.

Problem 2 This problem asks you to prove that semantic security implies security against key recovery attacks.

We say that a symmetric cipher \mathcal{E} is (t, ϵ) IND-CPA secure if there exists no t -time adversary that has advantage over ϵ in the following IND-CPA game against the Challenger.

1. The Challenger picks a key K from the keyspace of \mathcal{E} at uniform random.
2. The Challenger receives a set of plaintext messages sent by the adversary, encrypts these messages with key K , and returns the ciphertexts to the adversary.
3. The Challenger receives two distinct equal-length messages M_0, M_1 from the adversary, picks $b \in \{0, 1\}$ at uniform random, and returns $C = \mathcal{E}_K[M_b]$ to the adversary.
4. The Challenger receives a bit $b' \in \{0, 1\}$ from the adversary.
The adversary wins the game if and only if $b = b'$.

In other words, \mathcal{E} is (t, ϵ) IND-CPA secure when for any algorithm A with running time no more than t , $|\Pr[A \text{ wins the IND-CPA game}] - 0.5| \leq \epsilon$.

- a. (7 pts) Formalize a notion of security against chosen-plaintext key-recovery attackers for symmetric encryption schemes, similar to the above definition. That is, you should define when we say a cipher is (t, ϵ) KR-CPA secure. In this attack, the adversary is allowed to obtain ciphertexts of some messages chosen by the adversary, the adversary is then given a ciphertext, and asked to output the key under which the ciphertext is encrypted.
- b. (8 pts) Prove that if \mathcal{E} is (t, ϵ) IND-CPA secure, then \mathcal{E} is $(t - c, \epsilon)$ KR-CPA secure, for some small constant c .

Problem 3 Constructing hash functions from block ciphers.

Consider the Davies and Price construction of a hash function from a block cipher \mathcal{E} . A message x is divided into fixed-size blocks x_1, x_2, \dots, x_k . An Initial Vector is also used. The hash value of x is computed as follows.

$$\begin{aligned}
 H_0 &= \text{Initial Vector} \\
 H_i &= \mathcal{E}_{x_i}[H_{i-1}] \oplus H_{i-1} \text{ for } 1 \leq i \leq k \\
 H_k &\text{ is the hash value.}
 \end{aligned}$$

We use $h(x, y)$ to denote the hash value of message x when using y as the initial vector. For example, given two message blocks x_1, x_2 ,

$$h(x_1, y) = \mathcal{E}_{x_1}[y] \oplus y$$

$$h(x_1 || x_2, y) = h(x_2, h(x_1, y)) = \mathcal{E}_{x_2}[h(x_1, y)] \oplus h(x_1, y).$$

In this problem, we assume that DES is used as \mathcal{E} . Therefore, each message block has 56 bits and the initial vector and the hash value have 64 bits.

a. (10pts) An attacker is given a message x consisting of blocks $x_{1,2}, \dots, x_k$, an initial vector y and the hash code $h(x, y)$. Show that the attacker can easily find another initial vector y' and a message x' such that $h(x', y') = h(x, y)$.

Hint: Use the property about DES proved in Exercise 3.3.

b. (10 pts) Describe an algorithm that generates an initial vector y and an infinite sequence of messages x^1, x^2, x^3, \dots such that $h(x^1, y) = h(x^2, y) = h(x^3, y) = \dots$.

Hint: find a message block x_1 and a 64 bit block y such that $h(x_1, y) = y$.

c. (10 pts) Describe a variation of the above attack with expected running time $O(2^{32})$ to attack the hash function when the initial vector value is fixed to a value y_0 . The attack algorithm, when given y_0 , finds an infinite sequence of messages x^1, x^2, x^3, \dots such that $h(x^1, y_0) = h(x^2, y_0) = h(x^3, y_0) = \dots$.

Hint: find two message blocks x_1 and x_2 and a block y such that $h(x_1, y_0) = y = h(x_2, y_0)$.

Problem 4 (15 pts) Exercise 4.9 on Page 152

Problem 5 (30 pts) Exercise 4.13 on Page 153. [10 pts for each of (a), (b), (c)]

Typos in the book

- Line 2 of Exercise 4.13. “ $n \geq$ ” should be “ $n \geq 2$ ”.
- For Part (b), you should assume that $m > 2$ and y is different from x . Also, the forgery to be outputted should be computed as $4x'$ modulo 2^m .

Hint for Part (b): $(\mathbb{Z}_{2^m}, +, \cdot)$ is not a field, because $(\mathbb{Z}_{2^m}^*, \cdot)$ is not a group. For some $a \in \mathbb{Z}_{2^m}^*$, there may exist multiple $b \in \mathbb{Z}_{2^m}^*$ such that $a \cdot b \equiv 1 \pmod{2^m}$; for some $a \in \mathbb{Z}_{2^m}^*$, there may exist none.