

# HW #1: Symmetric Key Encryption

CS 996: Modern Cryptography  
Spring 2006

**[100pts] DUE 03/10/2007 (midnight)**

## **Problem 1 [10pts]**

What are the fundamental goals in information security? Give a practical scenario each where each of these goals are desired? Explain how cryptography can be used to achieve these goals?

## **Problem 2 [10pts]**

We studied various notions of security of a symmetric encryption scheme (against a passive attacker), namely, key recovery (KR), one-wayness (OW), indistinguishability (IND) and semantic security (SEM). State each of these notions (informally). What are the relations among these security notions (we studied some of these in the class)? Just state the relations.

Is one-wayness a stronger security notion than key recovery? Show why/why not. Give an example to illustrate where OW security might not be sufficient, but IND is.

## **Problem 3 [10pts]**

We discussed various active attacks on a symmetric encryption schemes, namely, chosen-plaintext attack (CPA), chosen-ciphertext attacks (CCA-1 and CCA-2). Describe each one of these attacks. Give a practical scenario where each such attack might be feasible to perform.

Show  $\text{IND-CCA2} \rightarrow \text{IND-CCA1} \rightarrow \text{IND-CPA}$ .

## **Problem 4 [10pts]**

We studied two different adversarial games to model the indistinguishability notion.:

- 1) The adversary chooses two messages to be challenged upon, and give them out to the oracle (possessing the encryption/decryption key). The oracle picks one of the messages at random and encrypts it and sends the ciphertext back to the adversary. If adversary can correctly tell which message was encrypted (with a probability greater than  $\frac{1}{2}$ ), it wins the game.

- 2) The adversary interacts with an oracle (possessing the encryption/decryption key), which is in either of two states: “World 0” and “World 1”. The adversary sends to the oracle two messages  $m_0, m_1$  to be challenged upon. If the oracle is in “World 0”, it replies back with an encryption of message  $m_0$  and if it is on “World 1”, it returns the encryption of message  $m_1$ . If the adversary can correctly tell which state (“World 0” or “World 1”) the oracle is in (with a probability better than  $1/2$ ), it wins the game.

Let's denote the advantages of the adversaries in the above two games as  $\text{Adv}(A_1)$  and  $\text{Adv}(A_2)$ . Show that  $\text{Adv}(A_1) = 2\text{Adv}(A_2) - 1$

### Problem 5 [10pts]

Show that DES encryption satisfies the complementation property, i.e. if  $C = \text{Enc}(K,P)$  then  $C' = \text{Enc}(K',P')$  ( $X'$  denotes the bitwise complement of  $X$ ).

You have to explain each and every step to prove this.

### Problem 6 [5pts]

We studied perfect cipher one-time pad (OTP). Is OTP a deterministic or a probabilistic encryption scheme, and why?

Is OTP secure under IND-CPA attack? Why or why not?

### Problem 7 [15pts]

- 1) [2.5pts] How many random functions are there in the random function family  $\text{Func}(4, 8)$ , for which domain consists of 4 elements and the range consists of 8 elements?
- 2) [2.5pts] How many random permutations are there in the random permutation family  $\text{Perm}(4,4)$  for which domain and range consist of 4 elements each?
- 3) [10pts]  $F$  is a secure PRF family, with key space of size  $k$  bits, domain of size  $l$  bits and range of size  $L$  bits. Is  $G$  defined as  $G(K,x) = F(K,x) || F(K,x')$  a secure PRF too, with key space of size  $k$  bits, domain of size  $l$  bits and range of size  $2L$  bits? Why or why not? (“||” denotes concatenation and  $X'$  denotes the bitwise complementation of  $X$ ).

### Problem 8 [10pts]

In the class, we showed that an encryption scheme instantiated with a PRF is secure in the sense of key recovery. Show a similar proof to illustrate that an encryption scheme instantiated with a PRP is also secure in the sense of key recovery.

### Problem 9 [10pts]

In the class, we showed that CBC-PRF, i.e., CBC mode of encryption instantiated with a PRF, is IND-CPA. Is ECB-PRF, i.e., ECB mode of encryption instantiated with a PRF, IND-CPA too? Why or why not?

**Problem 10 [10pts]**

- 1) **[5pts]** Is CBC-DES IND-CPA? Why or why not?
- 2) **[5pts]** Is CBC-DES IND-CCA? Why or why not?