CS 4920/5920 Applied Cryptography Spring 2018

Assignment 6

This homework is due at the beginning of class on April 25th.

Problem 1.

It is possible to use a hash function to construct a block cipher with a structure similar to DES. Given that a hash function is one way and a block cipher must be reversible (to decrypt), how is it possible? *Hint*: Identify a one-way function in DES.

Problem 2.

Let's use an encryption algorithm to construct a one-way hash function. Consider using RSA with a known key. Then process a message consisting of a sequence of blocks as follows: encrypt the first block, XOR the result with the second block and encrypt again, and so on. Show that this scheme is not secure by solving the following problem. You are given a two-block message B1, B2, and its hash

RSAH (B1, B2) = RSA (RSA(B1)$\oplus$B2)

Given an arbitrary block C1, choose C2 so that RSAH (C1, C2) = RSAH (B1, B2). Thus, the hash function does not satisfy weak collision resistance.

Problem 3.

At the beginning of Section 12.6 ("MACs Based on Block Ciphers: DAA and CMAC"), it was noted that given the CBC MAC of a one-block message X, say T = MAC(K ,X), the adversary immediately knows the CBC MAC for the two-block message $X \| (X \oplus T)$ since this is once again T. Justify this statement.

Problem 4.

In the discussion of subkey generation in CMAC, it states that the block cipher is applied to the block that consists entirely of 0 bits. The first subkey is derived from the resulting string by a left shift of one bit and, conditionally, by XORing a constant that depends on the block size. The second subkey is derived in the same manner from the first subkey.

a. What constants are needed for block sizes of 64 and 128 bits?
b. Explain how the left shift and XOR accomplishes the desired result.

Problem 5.

Consider the following protocol, designed to let A and B decide on a fresh, shared session key K'_{AB} .We assume that they already share a long-term key K_{AB}.

1. $A \rightarrow B$: A, N_A
2. $B \rightarrow A$: $E(K_{AB}, [N_A, K'_{AB}])$
3. $A \rightarrow B$: $E(K'_{AB}, N_A)$

a. We first try to understand the protocol designer's reasoning:

—Why would A and B believe after the protocol ran that they share K'_{AB} with the other party?

—Why would they believe that this shared key is fresh (i.e., associated with the current session as opposed to an outdated session)?

In both cases, you should explain both the reasons of both A and B, so your answer should complete the sentences (*Hint*: Use the parameters exchanged)

A believes that she shares K'_{AB} with B since...

B believes that he shares K'_{AB} with A since...

A believes that K'_{AB} is fresh since...

B believes that K'_{AB} is fresh since...

b. Assume now that A starts a run of this protocol with B. However, the connection is intercepted by the adversary C. Show how C can start a new run of the protocol using reflection, causing A to believe that she has agreed on a fresh key with B (in spite of the fact that she has only been communicating with C). Thus, in particular, the belief in (a) is false. *Hint*: C can initiate a new protocol in parallel to A's protocol.
c. Propose a modification of the protocol that prevents this attack.