Name: ____________
ID: ____________
Grade:____________
04/06/2011

Message Authentication Codes, Collision-Resistant Hash Functions, Block Ciphers, One-Way Function

4.1 Let F be a pseudorandom function. Show that the following MAC for messages of length $2n$ is insecure: The shared key is a random $k \in \{0,1\}^n$. To authenticate a message $m_1 \| m_2$ with $|m_1| = |m_2| = n$, compute the tag $\langle F_k(m_1), F_k(F_k(m_2)) \rangle$.

■

4.2 Show that the basic CBC-MAC construction is not secure when used to authenticate messages of different lengths.

■

4.3 Provide formal definitions for second pre-image resistance and pre-image resistance. Formally prove that any hash function that is collision resistant is second pre-image resistant, and that any hash function that is second pre-image resistant is pre-image resistant.

Definition of the second pre-image resistance:

Proof of its security based on collision resistant:

Definition of the pre-image resistance:

Proof of its security based on second pre-image resistant:

■

4.4 Let (Gen, H) be a collision-resistant hash function. Is $(\mathsf{Gen}, \hat{H})$ defined by $(\hat{H}^s(x) \overset{\text{def}}{=} H^s(H^s(x)))$ necessarily collision resistant? Prove your answer.

Proof:

■

4.5 For each of following modifications to the Merkle-Damgård transform, determine whether the result is collision resistant or not. If yes, provide a proof; if not, demonstrate an attack.

(a) Modify the construction so that the input length is not included at all (i.e, output z_B and not $z_{B+1} = h^s(z_B \| L)$).

(b) Modify the construction so that instead of outputting $z = h^s(z_B \| L)$, the algorithm outputs $z_B \| L$

(c) Instead of using an IV, just start the computation from x_1. That is, define $z_1 := x_1$ and then compute $z_i := h^s(z_{i-1} \| x_i)$ for $i = 2, \ldots, B+1$ and output z_{B+1} as before.

(d) Instead of using a fixed IV, set $z_0 := L$ and then compute $z_i := h^s(z_{i-1} \| x_i)$ for $i = 1, \ldots, B$ and output z_B.

■

5.1 In our attack on a two-round substitution-permutation network, we considered a block length of 64 bits and a network with 16 S-boxes that each take a 4-bit input.

(a) Repeat the analysis for the case of 8 S-boxes, each taking an 8-bit input. What is the complexity of the attack now?

(b) Repeat the analysis again with a 128-bit block length and 16 S-boxes that each take an 8-bit input.

(c) Does the block length make any difference?

■

5.2 What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases: (Show your analysis.)

(a) Each round function F outputs all 0s, regardless of the input.

(b) Each round function F is the identity function:

■

5.3 Show that DES has the property that $DES_k(x) = \overline{DES_{\overline{k}}(\overline{x})}$ for every key k and input x (where $\overline{z}$ denotes the bitwise complement of z). This is called the complementarity property of DES.

■

6.1 Prove that if f is a one-way function, then $g(x_1, x_2) = (f(x_1), x_2)$ where $|x_1| = |x_2|$ is also a one-way function. Observe that g fully reveals half of its input bits, but is nevertheless still one-way.

■