

Problem Set 6

Due on Thursday, November 30, 2006.

In the problems below, “textbook” refers to *Introduction to Cryptography with Coding Theory: Second Edition* by Trappe and Washington..

Problem 23: ElGamal Signatures

Textbook, problem 9.6.6.

Problem 24: Hash Functions

- (a) Suppose $h_1(x)$ and $h_2(x)$ are hash functions with the same length output strings. You are told that one of them is strongly collision-free, but you don’t know which. Use them to construct a hash function $H(x)$ that is definitely strongly collision-free, and prove that fact.
- (b) A general scheme was presented in section 82 of Lecture Notes 16 for constructing a hash function $H(m)$ from a function f , where f in turn is built from a symmetric cryptosystem with encryption function $E_k(b)$ according to one of four suggested schemas $f_1, \dots, f_4$. Suppose we use the XOR “one-time pad” cryptosystem, so $E_k(b) = k \oplus b$. Let $H_1(m), \dots, H_4(m)$ be the hash functions that result from the four suggested choices for f . Which of these do you think are strongly collision-free? Explain.

Problem 25: Simplified Feige-Fiat-Shamir Authentication Protocol

Happy Hacker decides to implement the simplified Feige-Fiat-Shamir authentication protocol presented in section 89 in Lecture Notes 17. Happy doesn’t see why it’s necessary to choose b at random, so he simply alternates bits, choosing first 0, then 1, then 0, then 1, and so forth. Give an algorithm that allows Irma, who does not know Alice’s secret s , to successfully impersonate Alice in 20 successive repetitions of the protocol.

Problem 26: Secret sharing basics

- (a) Textbook, problem 12.3.1.
- (b) Textbook, problem 12.3.5.

Problem 27: Secret sharing with cheater

Textbook, problem 12.3.8.