

Homework is due at the *start of class*, on the date listed above. **Problems numbered G# need only be completed by graduate students.**

0. *This problem is a reading exercise, and will not be graded.*

(a) Read Sections 5.2.1 and 5.2.2 from Stinson.

(b) Read the following portion from Section 5.3.1 of Stinson: from the paragraph beginning with “Suppose that x and y ...” in page 169, up to the description of Algorithm 5.5 in page 170.

1. Stinson, problem 5.3, page 219.

2. Stinson, problem 5.7, page 219.

3. Given two k -bit strings x and y , let $x \oplus y$ denote the bit-wise XOR of x and y leading to another k -bit string (just as is done in the one-time pad). Now consider the function $f : \{0, 1\}^k \times \{0, 1\}^k \rightarrow \{0, 1\}^k$ given by $f(x, y) = x \oplus y$. Show that f is **not** a one-way function.

G1. (**For graduate students only.**) Show that an one-way function exists if and only if a weak one-way function exists. (**Hints:** If A and B are independent events, then $\Pr[A \text{ and } B] = \Pr[A] \times \Pr[B]$. Also, the inequality $1 + x \leq e^x$ which holds for all real numbers x , may be of use.)

G2. (**For graduate students only.**) Let A_t denote the set of integers $\{0, 1, \dots, 2^t - 1\}$. Consider the function $f : A_k \times A_k \rightarrow A_{4k+1}$, given by $f(x, y) = x^4 + y$. Show that f is **not** a one-way function.