

Homework is due at the *start of class*, on the date listed above.

1. Problem 7.14 from pages 313–314 of Stinson.
2. Suppose $f : A \rightarrow B$ is a random function, implemented by a random oracle. We are given a random $y \in B$, and want to find some $x \in A$ (if any) such that $f(x) = y$. We do so by choosing t random elements $x_1, x_2, \dots, x_t \in A$ without replacement, and use the oracle to see if $f(x_i) = y$ for some i ; if the answer from the oracle was always “no”, we just give up after the t queries to the oracle. What is the probability that we successfully got an answer?

How does the above change if $f : A \rightarrow A$ is a random *permutation*?

3. **(For graduate students, and extra credit for undergraduate students.)** Read about the El Gamal signature scheme from pages 280–282 of Stinson. (A *primitive element* of Z_p^* is a generator of Z_p^* .) Do parts (a) and (b) of problem 7.6 from page 312 of Stinson.