Harvard University Salil Vadhan

CS 127: Introduction to Cryptography

Quiz I Practice Problems

September 29, 2013

Justify all of your answers. This also applies to questions which are not purely mathematical, for which you should back up your answers with mathematical explanations. You may assume all results proven (or stated as a fact) in class or on the problem sets. This set of practice problems is roughly twice the length of the actual quiz.

Problem 1.

1. State the definition of the one-time pad encryption scheme for n-bit messages. Your specification should include: the message space, the ciphertext space, the key space, and functions Gen, Enc_k and Dec_k.

2. Why is the one-time pad not commonly used in practice?

Problem 2. **(KL exercise 2.6, modified)** When using the one-time pad with the key 0^n, the entire message is sent in the clear. It has therefore been suggested that the one-time pad be modified by only encrypting with keys $k \neq 0^n$ chosen uniformly at random. Is the resulting scheme still perfectly secret? What is the smallest $\varepsilon \geq 0$ for which this scheme has statistically ε-indistinguishable encryptions? Would we want to make such a modification in practice?

Problem 3. For each of the following, answer whether it is TRUE or FALSE for each of the notions of perfect secrecy, statistical security, and computational security.

1. Assumes an adversary with limited computation time

2. Provides privacy for each individual bit of a message

3. May allow an adversary to "break" the scheme with some small probability

4. Is achievable assuming $\mathbf{P} \neq \mathbf{NP}$

Problem 4. Each day, a satellite sends a single encrypted message back to Earth using a 128-bit one-time pad, with a fresh key for each day. Each message consists of a 64-bit timestamp (the number of seconds since 1970 in binary) and a 64-bit payload (the satellite's current sensor readings). A hacker claims that, by listening in on the communication, she is able to determine 10 bits of the given day's 128-bit message. Is the hacker's claim plausible? Does the scheme satisfy our definition of perfect secrecy?

Problem 5. **(KL exercise 3.7)** Show that if G is not a pseudorandom generator, then $\mathsf{Enc}_k(m) = G(k) \oplus m$ does not have indistinguishable encryptions.

Problem 6.

1. Give the definition of a pseudorandom generator.

2. Suppose $G : \{0,1\}^* \rightarrow \{0,1\}^*$ is a pseudorandom generator. Which of the following G' is *necessarily* a pseudorandom generator for every pseudorandom generator G? Justify your answer (e.g., by a reducibility argument or a counterexample).

   (a) $G'(x) = G(x)b(x)$, where $b(x)$ is the XOR of all the bits of $G(x)$.

   (b) $G'(x) = G(x0^{|x|})$.

   (c) $G'(x) =$ the first $|x| + 1$ bits of $G(x)$