

Homework 2

Instructor: Anna Lysyanskaya

Due: Feb 4, 2009

Problem 1: Shannon security

Recall the Shannon definition of security for a cryptosystem.

Let G be an algorithm that generates the secret key s and gives it to Alice and Bob. Let E and D be the encryption and decryption algorithms. Let us think of the plaintext message m as drawn from some probability distribution M . Let $c = E(m, s)$ be a ciphertext.

Definition 1 (Shannon-security). (G, E, D) constitute a Shannon-secure cryptosystem if for all messages $m \in M$, and for all possible ciphertexts c , $\Pr[m] = \Pr[m|c]$.

In other words, Shannon-security says that all that the adversary knows to begin with, is that the message came from the message space M . Seeing the ciphertext did not make him any the wiser.

a. Consider the following definition:

Definition 2 (A-security). (G, E, D) constitute an A-secure cryptosystem if for all messages $m \in M$, and for all possible ciphertexts c , $\Pr[c] = \Pr[c|m]$.

Is A-security equivalent to the original Shannon definition? Prove or disprove your answer.

b. Suppose we have a Shannon-secure cryptosystem, such that for some distribution M of messages, \forall messages m_0, m_1, \forall possible ciphertexts $c, \Pr[m_0|c] = \Pr[m_1|c]$. What (if anything) can you infer about distribution M ? Prove your answer.

Problem 2: Probability Review

Larry the lottery man is advertising a new lottery system. Here are the lottery rules:

- The cost of a lottery ticket is \$10.
- With probability .35, your winnings are \$20 or more.
- With probability .15, your winnings are \$25 or more.
- With probability .1, your winnings are \$30 or more.

Larry says: "If you buy the ticket, your chance of losing money is only $(1 - 0.35) \cdot (1 - 0.15) \cdot (1 - 0.10) = 0.497$. You always win at least as much as your bet. So, on average, you win more than you lose. So you must play!"

Can it be possible that this lottery is as good as he says? Is there a flaw in his argument? How likely are you to win? What are your expected winnings?

Problem 3: Negligible functions

In cryptography, we usually define security by requiring that the probability of some undesirable event (e.g. Eve guesses the message) to be so small that one would never notice it. To that end, we define a negligible function as follows:

Definition 3. (*Negligible function*) A function $\nu(k) : \mathbb{N} \mapsto [0, 1]$ is called negligible if for all polynomials p , there exists some $k_0 \geq 1$ such that for all $k > k_0$, $\nu(k) < |1/p(k)|$.

In this problem we will develop some intuition for this useful concept and how to work with it.

- a. Give an example of a negligible function $\nu(k)$ where $\nu(k) > 0$ for all k .
- b. Suppose that ν , is a negligible function. Let p be a polynomial such that $p(k) \geq 0$ for all $k > 0$. Which of the following functions are negligible: (give yes/no)
 - $\nu(p(k))$.
 - $\nu_1(k) * \nu_2(k)$ where both ν_1 and ν_2 are negligible.
 - $\nu(k) * p(k)$.
 - $\sum_{i=1}^{p(k)} \nu_i(k)$ where each ν_i is a negligible function.
 - $\nu_1(k)/\nu_2(k)$ where both ν_1 and ν_2 are negligible.
 - $\frac{1}{p(k)} - \nu(k)$.
- c. Suppose that $\epsilon : \mathbb{N} \mapsto [0, 1]$ is not a negligible function. Does it follow that for some polynomial p (where $p(k) > 0$ for all k) and some k_0 , $\epsilon(k) > 1/p(k)$ for all $k > k_0$? If your answer is yes, prove it. If your answer is no, give a counter-example.

Problem 4: Fun With One Way Functions (worth 50 points!)

Suppose that $f(x)$ is a one-way function. Let $|x|$ denote the length of binary string x . We let \circ denote the concatenation operator. Similarly (\circ) is the parse operator such that when we parse $x = x_2(\circ)x_1$ we get $\|x_1| - |x_2| \leq 1$ (i.e. (\circ) splits the string x roughly in half).

For each of the following, use a reduction to prove it is a one-way function or give a counterexample showing it is not a one-way function. Function f here is *length-preserving*, which means that $|f(x)| = |x|$.

- a. $f_a(x) = f(x_1) \circ x_2$, where $x = x_1(\circ)x_2$.
- b. $f_b(x) = x_1 \circ f(x)$, where $x = x_1(\circ)x_2$.
- c. $f_c(x) = \begin{cases} 0^{|x_1|} \circ f(x_2) & \text{if } x_1 \neq 0^{|x_1|} \\ f_c(x) = 0^{|x|} & \text{otherwise} \end{cases}$ where $x = x_1(\circ)x_2$.