Project 3 : Applied Cryptography

CS 475: Computer and Network Security
Project 3 Due: May 26, 2012 11:59 pm EST

May 13, 2012

Problem 1: Overclockers Anonymous [5 pts]

Assume a cryptographic algorithm that is linear in the length of the key to perform "good guy operations", e.g., encryption, decryption, key generation, integrity check generation, integrity check verification; and that it is exponential in the length of the key to perform "bad guy operations", e.g., brute force breaking. Suppose advances in computation make computers an order of magnitude faster. Does this work to the advantage of the good guys, the bad guys, or neither? Justify your answer.

Problem 2. Confidentiality in the face of keyloggers [20 pts]

Suppose that an adversary can see all the keys that you type on your keyboard. Is it possible for you to securely type in a password to a program that is running on your machine? You can assume that the adversary can only log your keystrokes, and that you can make small modifications to the program which accepts your password. Either describe a method or argue why it is impossible. [Note, it would be best if you do not require a third-party device, such as a calculator, to complete logins.]

Problem 3. Hashtastic Functions [15 pts]

Bob has two hash functions, f and g. He knows that one of them is collision-resistant (and the other isn't), but he's not sure which is which. He wants to create a new hash function h which is definitely collision-resistant. Evaluate each of the following proposals, and either give a proof that it is definitely collision-resistant, or describe a counterexample (as usual, the $\circ$ symbol denotes concatenation):

1. $h(x) = f(x) \circ g(x)$
2. $h(x) = f(g(x))$
3. $h(x) = f(g(x)) \circ g(f(x))$

Problem 4. Hashes Everywhere [15 pts]

Estimate the probability that there are two non-identical files, somewhere on the planet Earth, right now, that have the same MD5 hash code. Do the same for SHA-1. State your assumptions and cite all references used.

Problem 5. Two-Timing Pads [45 pts]

In this problem, we will explore why it's never a good idea to reuse your one-time pads. I've provided six messages encrypted with three one-time pads (available on the course website).

The problem has three parts, each worth 15 points.

1. Discuss your approach to solving this problem. Consider the ASCII encoding system, the mathematical properties of exclusive-or, predictability of human and computer languages, and any other factors that will help you solve this problem.
2. Determine which pairs of ciphertext were encrypted using the same "one-time" pads.

3. Report the six plaintexts.

Hints:

- Each pad was used exactly twice.
- One of the messages is code, one of the messages is song lyrics, and one of the messages is a Shakespeare quotation. The other three are other memorable phrases.
- The following links may be helpful:
  - One Time Pad Vernam Cipher FAQ: http://www.ranum.com/security/computer_security/papers/otp-faq/
  - The NSA's VENONA project: http://www.nsa.gov/public_info/declass/venona/