Reading

Read RFC 3972, Cryptographically-generated addresses.

Objectives

The purpose of this assignment is to help you understand the issues associated with self-certifying network addresses.

Writeup

For Part One, write out (neatly!) your answers to the questions. For Parts Two and Three, prepare a detailed (and neat!) laboratory-type written report: tell exactly what you did, what tools you used, and what the results were. (Remember that writing such reports is a crucial part of good forensics.)

Part One

Answer the following questions:

a. For a cryptographically-generated address (CGA) with security parameter 1, according to the RFC how many leading zeros should the result of Hash 1 have?

b. What fraction of all hash values have that many leading zeros? (Note: the answer to this question is independent of the size of the hash output, assuming it is large enough to have that many zeros.)

c. What is the advantage of the CGA approach (security parameter) compared with the simpler approach of using a larger hash? What is the disadvantage compared to the simpler approach?

Part Two

a. Find several (at least three) distinct inputs for which the outputs of SHA-1 have at least 16 leading zeroes, and report the input/output pairs. How long did it take you to find those values?

b. Find an input for which the output of SHA-1 has at least 24 leading zeroes, and report the input/output pair. How long did it take you?

Part Three

Find a parameter block (as described in the CGA RFC) containing a valid RSA public key (i.e., there exists a valid private key that works with the public key under the RSA algorithm), for which the output under SHA-1 has 16 leading zeros. How long did it take you? (Note: If you don’t know how to write a program to do this, talk to the instructor about another possible way to do it.)