CS346 Cryptography Investigation
Due: April 18, 2012

Brent Waters

Overview

The purpose of this Research Investigation project is 3-fold:

1. To have fun exploring a new and further out topic in cryptography.
2. To learn and experience how to gather information and learn about a topic without being given explicit references.

For this "Research Investigation" you will write 3 pages (more is allowed) on a cryptography topic of your choice. The topic, style and content of the write up will be largely up to each student's discretion. The main goal should be to inform the reader about the topic: What is it about? What makes it interesting or challenging? What is new? Imagine writing to the target audience of a fellow student in the class.

You are not required or expected to obtain new research results as part of this project. However, all material must be written up by yourself. You are not allowed to copy any text verbatim.

You may work with 1 partner in this project and turn in 1 writeup — this is different from the policy of our problem sets where you must write up the solutions yourself.

There are a variety of different directions to go with this. Some could be about learning about a recent cryptography or security related current news item. Another could be to learn what you can about an advanced area in cryptography. The choice is basically yours. A few possible directions are listed below, but you are not limited to them.

Possible Topics

1. How fast is cryptography? What are options for cryptography accelerated hardware? Smartcards?
2. What are the most efficient algorithms for factoring integers? What is the RSA factoring challenge? How does this impact our choice for the size of parameters in practice.
3. What is the Linux Debian random number generator and what went wrong with it?

4. Try to implement some of our crypto using the Big Number package in Java. Tell us about your experiences.
5. What is a "coldboot" attack and what did we learn about it?
6. What happened with the RSA SecureID token? (Note the RSA SecureID token has nothing to do with the RSA algorithm.)
7. What is PKCS#1 and what went wrong?

More Crypto/ Theoretical

1. What is quantum computing? What does it mean for cryptography?
2. What are elliptic curves and why use them in cryptography? What does the NSA say about them?
3. What is Secure Multi-party computation? What are recent advances?
4. Who is Amit Sahai and what is something that he works on? Should we be concerned?
5. What are anonymous credentials and where are they being used?
6. What is homomorphic encryption? What are some of the recent advances and why are they exciting?
7. Can public key cryptography be based on symmetric key cryptography? Are there obstacles?
8. What is Identity-Based Encryption? What is its history?
9. What are Merkle Puzzles and how do they work?
10. What are time-lock puzzles and what new has been done with them?