95-702 Distributed Systems

Lecture 12: RSA

Plan for today:

- Introduce RSA and a toy example using small numbers. This is from Introduction to Algorithms by Cormen, Leiserson and Rivest

- Describe an interesting cryptographic protocol and its limitations.
  This is from Applied Cryptography by Bruce Schneier.

- Show how RSA cryptography can be done in Java. See the Java Cryptograhy API.

Purpose of RSA

Privacy: to send encrypted messages over an insecure channel.

Authentication: To digitally sign messages.

RSA was not the first public key approach.
Public key cryptography was first introduced by Diffie and Hellman in 1976.

RSA was developed by Rivest, Shamir, and Aldeman in 1977
It's probably safe to call public key cryptography revolutionary.