Lecture 9: Security of RSA

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE.

Because both the system's privacy and the security of digital money depend on encryption, a breakthrough in mathematics or computer science that defeats the cryptographic system could be a disaster. The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers. Any person or organization possessing this power could counterfeit money, penetrate any personal, corporate, or government file, and possibly even undermine the security of nations.

Bill Gates, *The Road Ahead*

CS588: Security and Privacy
University of Virginia
Computer Science

David Evans
http://www.cs.virginia.edu/~evans

Menu

- Finding Big Pseudo Primes
- Security of RSA
  - Factoring

Properties of E and D

Trap-door one way function:

✓ 1. $D(E(M)) = M$

➡ 2. E and D are easy to compute.

3. Revealing E doesn't reveal an easy way to compute D

Trap-door one way permutation: also

4. $E(D(M)) = M$