Lecture 8:
Security of RSA

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE.

CS551: Security and Privacy
University of Virginia
Computer Science

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

Menu

- (Anonymous) Pop Quiz
- Security of RSA
  - Factoring
- Public Key Infrastructures

Properties of E and D

- Trap-door one way function:
  - ✓ $D(E(M)) = M$
  - ✓ E and D are easy to compute.
  - → Revealing E doesn't reveal an easy way to compute D (next time)
- Trap-door one way permutation: also
  - ✓ $E(D(M)) = M$

Are there other functions that have properties 1, 2 and 4?