The RSA Trapdoor Permutation

Dan Boneh
Stanford University

Review: arithmetic mod composites

- Let $N = p \cdot q$ where p,q are prime
- Notation: $Z_N = \{0,1,2,\ldots,N-1\}$

  $(Z_N)^* = \{\text{invertible elements in } Z_N\}$
- Facts:
  - $x \in Z_N$ is in $(Z_N)^* \iff \gcd(x,N) = 1$
  - Number of elements in $(Z_N)^*$ is $\varphi(N) = (p-1)(q-1)$
- Euler's thm: $\forall\, x \in (Z_N)^* \;:\; x^{\varphi(N)} = 1$

The RSA trapdoor permutation

- First published:
  - Scientific American, Aug. 1977.
    (after some censorship entanglements)

- Currently the "work horse" of Internet security:
  - Most Public Key Infrastructure (PKI) products.
  - SSL/TLS: Certificates and key-exchange.
  - Secure e-mail: PGP, Outlook, …