The RSA Cryptosystem

Dan Boneh
Stanford University

The RSA cryptosystem

- 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, ...

The RSA trapdoor 1-to-1 function

- **Parameters:** N=pq. N ≈1024 bits. p,q ≈512 bits.
  e – encryption exponent. gcd(e, φ(N)) = 1 .

- **1-to-1 function:** $\mathbf{RSA(M) = M^e \pmod N}$ where $M \in Z_N^*$

- **Trapdoor:** **d** – decryption exponent.
  Where $e \cdot \mathbf{d} = 1 \pmod{\varphi(N)}$

- **Inversion:** $\mathbf{RSA(M)}^{\mathbf{d}} = M^{ed} = M^{k\varphi(N)+1} = \mathbf{M} \pmod N$

- **(n,e,t,ε)-RSA Assumption:** For any t-time alg. A:

$$\Pr\left[\ A(N,e,x) = x^{1/e}\ (N)\ :\ p,q \xleftarrow{R} \text{primes, } n\text{-bit}\ \right] < \varepsilon$$

$N \leftarrow pq \quad x \leftarrow Z_N^*$