CSE 543 - Computer Security

Lecture 5 - Cryptography II
September 19, 2006
URL: http://www.cse.psu.edu/~tjaeger/cse543-f06/

RSA (Rivest, Shamir, Adelman)

- A dominant public key algorithm
  - The algorithm itself is conceptually simple
  - Why it is secure is very deep (number theory)
  - Use properties of exponentiation modulo a product of large primes

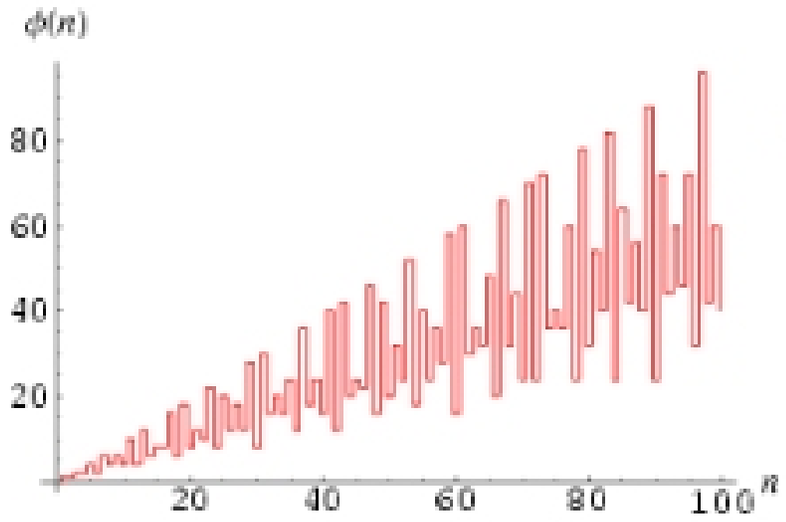
"A method for obtaining Digital Signatures and Public Key Cryptosystems“, Communications of the ACM, Feb., 1978 21(2) pages 120-126.

RSA Key Generation

- Pick two large primes p and q
- Calculate n = pq
- Pick e such that it is relatively prime to phi(n) = (q-1)(p-1)
  - "Euler's Totient Function"
- $d \sim= e^{-1} \bmod phi(n)$

or

de mod phi(n) = 1



1. p=3, q=11
2. n = 3*11 = 33
3. phi(n) = (2*10) = 20
4. e = 7 | GCD(20,7) = 1
   "Euclid's Algorithm"
5. d = 7-1 mod 20
   d = 7 mod 20 = 1
   d = 3