RSA

Hyoungshick Kim
Department of Software
College of Software
Sungkyunkwan University

The RSA problem

- Here: group $\mathbb{Z}^*_N$ of order $\phi(N)$
- Choose e with $\gcd(e, \phi(N)) = 1$
  - Raising to the e-th power is a permutation on $\mathbb{Z}^*_N$!
- If $ed = 1 \bmod \phi(N)$, raising to the d-th power is the *inverse* of raising to the e-th power
  - i.e., $(x^e)^d = x \bmod N$, $(x^d)^e = x \bmod N$
  - x^d is the *e-th root of x modulo N*

The RSA problem

- If p, q are known:
  - $\Rightarrow \phi(N)$ can be computed
  - $\Rightarrow d = e^{-1} \bmod \phi(N)$ can be computed
  - $\Rightarrow$ possible to compute e-th roots modulo N
- If p, q are *not* known:
  - $\Rightarrow$ computing $\phi(N)$ is as hard as factoring N
  - $\Rightarrow$ co

Very useful for public-key cryptography!

The RSA assumption (informal)

- Informally: given N and e, hard to compute the e-th root of a uniform element $y \in \mathbb{Z}^*_N$

Implementing RSA

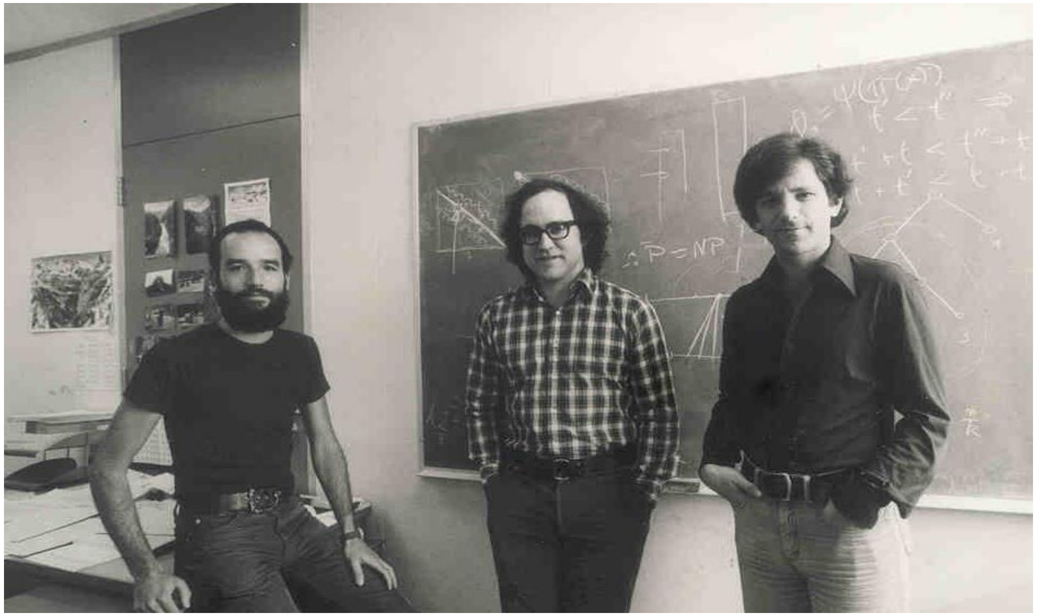
- One way to implement RSA:
  - Generate uniform n-bit primes p, q
  - Set $N := pq$
  - Choose arbitrary e with $\gcd(e, \phi(N))=1$
  - Compute $d := [e^{-1} \bmod \phi(N)]$
  - Output (N, e, d)

Implementing RSA

- Choice of e?
  - Does not seem to affect hardness of the RSA problem
  - e = 3, $2^{16} + 1$ (1 0000 0000 0000 0001; i.e., efficient for square and multiply; prime number) for efficient exponentiation

RSA public key crypto

- Proposed in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman at MIT
- It is believed to be secure and still widely used



Shamir *Rivest* *Adleman*

(Plain) RSA crypto system

- Private key is two large primes p, q or d
- Public key is $n = pq$ and public exponent e
  - e is a relatively prime to $\phi(N)$ (= $(p-1)(q-1)$)
  - find d where $de = 1 \pmod{\phi(N)}$
- Encryption: $c = m^e \pmod{n}$
- Decryption: $m = c^d \pmod{n}$
  - $m^{ed} = m^{(1+k(p-1)(q-1)) \bmod (p-1)(q-1)} = m$

Simple RSA example (1)

- Select large(?) primes $p = 11, q = 3$
- Then $N = pq = 33$ and $(p-1)(q-1) = 20$
- Choose $e = 3$ (relatively prime to 20)
- Find d such that $ed = 1 \bmod 20$
  - We find that $d = 7$ works
- **Public key:** $(N, e) = (33, 3)$
- **Private key:** $d = 7$

Simple RSA example (2)

- **Public key:** $(N, e) = (33, 3)$
- **Private key:** $d = 7$
- Suppose message $M = 8$
- Ciphertext C is computed as

$$C = M^e \bmod N = 8^3 = 512 = 17 \bmod 33$$

- Decrypt C to recover the message M by

$$\begin{aligned} M = C^d \bmod N &= 17^7 = 410{,}338{,}673 \\ &= 12{,}434{,}505 * 33 + 8 = 8 \bmod 33 \end{aligned}$$

Security of (plain) RSA crypto

- This scheme is deterministic
  - Cannot be CPA-secure! (i.e., CPA-secure crypto must be randomized)
- RSA assumption only refers to hardness of computing the e^{th} roots of uniform C
  - C is not uniform unless M is
  - Partial information about the e^{th} root may be leaked

Plain RSA should never be used!

Questions?


Sungkyunkwan
Campus
Social
Graduate
campus
Sciences
University
Seoul
Natural
Suwon
School
Korean
established
university
edit
English
constructed
Professors
Confucian
Global
Engineering
located
Joseon
Building
Institute
Education
Humanities
lecturers
schools
Science
Administration
Academic
ASLE-Korea
Advanced
Language
Samsung
Zone
Business
also
two
four
campuses
storeys
city
Hall
Course