The RSA Cryptosystem

Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
Email: gianluca.dini@.unipi.it
Version: 17/03/25

1

The RSA Cryptosystem

BASICS

Mar-25 The RSA Cryptosystem 2

2

RSA in a nutshell

- Rivest-Shamir-Adleman, 1978
  - Rivest, R.; Shamir, A.; Adleman, L. A Method for Obtaining [Digital Signatures and Public-Key Cryptosystems](), *Communications of the ACM,* 21 (2): 120–126, February 1978.
- The most widely used asymmetric crypto-system
- Patented until 2000 in US
- Many applications
  - Encryption of small pieces (e.g., key transport)
  - Digital Signatures
- Underlying one-way function: integer factorization problem

As long as it is difficult to factorise very large numbers, RSA can be considered secure

3

2048 keys are now used because nowadays it is possible to bruteforce a 784 bits keys but not a 2048.

RSA one-way function

- One-way function y = f(x)
  - y = f(x) is easy
  - x = $f^{-1}(y)$ is hard
- RSA one-way function
  - Multiplication is easy
  - Factoring is hard

4

Mathematical setting

UNIVERSITÀ DI PISA

- RSA encryption and decryption is done in the integer ring $\mathbb{Z}_n = \{0, 1, \ldots, n\text{-}1\}$ We use modular arithmetics.
  - PT and CT are elements in $\mathbb{Z}_n$
  - Modular computation plays a central role

- 1st diff. with symmetric encryption
  - PT and CT are just sequences of bytes, while here they are integer numbers.

Mar-25 The RSA Cryptosystem 5

5

Modular arithmetic

UNIVERSITÀ DI PISA

- C. Paar, J. Pelzl. *Understanding Cryptography*
  - 1.4.1 Modular Arithmetic
  - 1.4.2 Integer Rings
  - 6.3 Essential Number Theory for Public-Key Algorithms
    - 6.3.1 Euclidean Algorithm
    - 6.3.2 Extended Euclidean Algorithm
    - 6.3.3 Euler's Phi Function
    - 6.3.4 Fermat's Little Theorem and Euler's Theorem

Mar-25 The RSA Cryptosystem 6

6

Key Generation

THEY MUST BE RANDOM
(OTHERWISE ATTACKABLE)
(Around 300 digit)

1. Choose two large, distinct primes p, q
2. Compute modulus $n = p \times q$ n is called the modulus
3. Compute Euler's Phi function $\phi(n) = (p-1) \times (q-1)$
4. Randomly select the public (encryption) exponent e, $1 < e < \phi(n)$, s.t. $\gcd(e, \phi(n)) = 1$
5. Compute the unique private (decryption) exponent d, $1 < d < \phi$, such that $e \cdot d \equiv 1 \pmod{\phi}$ ① $\phi(n)$
6. Private key = (d, n), Public key = (e, n)

① Solve equation for d! $e \cdot d \equiv 1 \bmod \phi = 1 + z\phi$ for some z

Mar-25 The RSA Cryptosystem 7

7

RSA Key Generation

- Comments
  - Primes p and q are 100÷200 decimal digits
    - Nowadays, p and q are 1024 bit
  - Condition $\gcd(e, \Phi(n)) = 1$ guarantees that *d* exists and is unique. d is the inverse of e
  - At the end of key generation, p and q must be deleted and ϕ too
  - Two parts of the algorithm are nontrivial:
    - Step 1
    - Steps 4-5 (step 5 is crucial for RSA correctness)

Step 1 requires me to generate large prime numbers that must be random.
Step 4 is "difficult" because we select e in such a way to speed up encryption

Mar-25 The RSA Cryptosystem 8

8

RSA Encryption and Decryption Algorithm

- Encryption algorithm: to generate the ciphertext y from the plaintext x ∈ [0, n – 1]
  - Obtain receiver's authentic public key (n, e)
  - Compute $\mathbf{y = x^e \bmod n}$
- Decryption algorithm: to obtain the plaintext x from the ciphertext y ∈ [0, n - 1]
  - Compute $\mathbf{x = y^d \bmod n}$

Mar-25 The RSA Cryptosystem 9

9

Example with artificially small numbers

Key generation

- Let p = 47 e q = 71
  n = p × q = 3337
  ϕ= (p-1) × (q-1)= 46 × 70 = 3220
- Let e = 79
  ed = 1 mod ϕ
  79 × d = 1 mod 3220
  d = 1019

Encryption

Let m = 9666683 message is longer than modulus

Divide m into blocks m_i < n I apply a sort of ECB

m_1 = 966; m_2 = 668; m_3 = 3

Compute

$c_1 = 966^{79} \bmod 3337 = 2276$

$c_2 = 668^{79} \bmod 3337 = 2423$

$c_3 = 3^{79} \bmod 3337 = 158$

$c = c_1c_2c_3$ = 2276 2423 158

Decryption

$m_1 = 2276^{1019} \bmod 3337 = 966$

$m_2 = 2423^{1019} \bmod 3337 = 668$

$m_3 = 158^{1019} \bmod 3337 = 3$

m = 966 668 3

For more efficient to use hybrid symmetric + asymm. scheme

Mar-25 The RSA Cryptosystem 10

10