

RSA encryption

SET07106 Mathematics for Software Engineering

School of Computing
Edinburgh Napier University
Module Leader: Uta Priss

2010

RSA encryption

RSA algorithm named after
Rivest, Shamir and Adleman (the inventors of the algorithm).

First described in 1978.

Magician's number game

The RSA algorithm is a bit like a magician's number game.

A magician asks you to think of a number (m), then applies some calculations (add, multiply, etc) using numbers (e, n) which the magician gives to you. Finally, the magician asks you to state the result c .

The magician then uses a secret formula (using d) to retrieve m .

Public and private keys

The RSA algorithm uses

- ▶ message m which is encoded into c
- ▶ public key e, n for encryption
- ▶ private key d for decryption

Publicly known: e, n, c .

Secret, known to sender and recipient: m

Secret, only known to recipient: d, p, q .

Integer factorisation

It is difficult to find factors of large numbers.

Problem: $n = pq$ (p and q are prime numbers)

6 =

Integer factorisation

It is difficult to find factors of large numbers.

Problem: $n = pq$ (p and q are prime numbers)

$$6 = 2 \times 3$$

$$55 =$$

Integer factorisation

It is difficult to find factors of large numbers.

Problem: $n = pq$ (p and q are prime numbers)

$$6 = 2 \times 3$$

$$55 = 5 \times 11$$

$$8633 =$$

Integer factorisation

It is difficult to find factors of large numbers.

Problem: $n = pq$ (p and q are prime numbers)

$$6 = 2 \times 3$$

$$55 = 5 \times 11$$

$$8633 = 89 \times 97$$

n has:	or:	it takes:
300 bits	100 digits	hours
600 bits	200 digits	months
1024 bits	300 digits	currently not possible
2048 bits	600 digits	currently not possible

Algorithm: General Number Field Sieve

Modulo calculations (RSA problem)

Given: $m^e \equiv c \pmod{n}$

Problem: e, c, n are known. m is unknown.

(Example: $4^3 \equiv 9 \pmod{55}$)

Modulo calculations (RSA problem)

Given: $m^e \equiv c \pmod{n}$

Problem: e, c, n are known. m is unknown.

(Example: $4^3 \equiv 9 \pmod{55}$)

For $m^e = c$, one would just compute the e-th root: $\sqrt[e]{c} = m$.

($4^3 = 64$; calculate: $\sqrt[3]{64} = 4$)

Modulo calculations (RSA problem)

Given: $m^e \equiv c \pmod{n}$

Problem: e, c, n are known. m is unknown.

(Example: $4^3 \equiv 9 \pmod{55}$)

For $m^e = c$, one would just compute the e-th root: $\sqrt[e]{c} = m$.

($4^3 = 64$; calculate: $\sqrt[3]{64} = 4$)

But this does not work if modulo is involved:

$$\sqrt[3]{9 \pmod{55}} = ?$$

Modulo calculations (RSA problem)

Given: $m^e \equiv c \pmod{n}$

Problem: e, c, n are known. m is unknown.

Example:

$$15^3 = 3375 \equiv 20 \pmod{55}$$

Try all possibilities:

$$1^3 \equiv 1 \pmod{55}$$

$$2^3 \equiv 8 \pmod{55}$$

$$3^3 \equiv 27 \pmod{55}$$

$$4^3 \equiv 9 \pmod{55}$$

...

$$15^3 \equiv 20 \pmod{55}$$

Solving the RSA problem

The RSA problem can be solved, if it is known that $n = pq$.

$$m^3 = 15^3 = 3375 \equiv 20 \pmod{55} \equiv 20 \pmod{5 \times 11}$$

Find: d so that $3d \equiv 1 \pmod{(5-1)(11-1)} \equiv 1 \pmod{40}$.

Solving the RSA problem

The RSA problem can be solved, if it is known that $n = pq$.

$$m^3 = 15^3 = 3375 \equiv 20 \pmod{55} \equiv 20 \pmod{5 \times 11}$$

Find: d so that $3d \equiv 1 \pmod{(5-1)(11-1)} \equiv 1 \pmod{40}$.

$$d = 27; \quad 3 \times 27 \equiv 1 \pmod{40}$$

Now m can be retrieved with this formula:

$$20^{27} \equiv 15 \pmod{55}$$

(The formulas use Euler's totient and Euler's theorem from Number Theory.)

Breaking RSA encryption?

As long as there is no fast solution for finding

$$n = pq$$

RSA encryption is safe.

RSA encryption

$$m^e \equiv c \pmod{n}$$

- ▶ Secret message: m
- ▶ Code, encrypted text: c
- ▶ Public key: e, n

The key for encryption is publicly known.

RSA decryption

Decryption uses the private key d .

$$c^d \equiv m \pmod{n}$$

As long as it is not possible to discover p and q with $n = pq$, it is not possible to find d or to decrypt m .

Security conditions

- ▶ n should have at least 300 digits (possibly more in the future)
- ▶ p, q should be randomly chosen, of similar length, not too close to each other
- ▶ $e \leq 3$ is not a good idea, in particular if the message is very short (unless the message is padded).
- ▶ Without padding, RSA can be broken by encrypting likely plain texts and comparing them with an encoded message.