RSA Public Key Cryptosystem

Suppose
N letter alphabet ($N = 26$)

plaintext message units $\longleftrightarrow$ integers

The cryptosystem:

- each user chooses two random primes p, q, together with a random integer e with

  $\gcd(e, p-1) = 1$

  $\gcd(e, q-1) = 1$.

- Each user computes

  $$n = pq$$

  and publishes the enciphering key $K_E = (n, e)$

- Each user computes (using Euclid's algorithm)

$$d = e^{-1} \bmod \phi(n)$$

Note $\phi(n) = \phi(pq)$

$= \phi(p)\,\phi(q)$

$= (p-1)(q-1)$

The deciphering key

$k_D = (n, d)$

is kept secret.

- The enciphering function is

$f_{(n,e)} : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \quad x \longmapsto x^e$

Proposition

$$(x^e)^d \equiv x \bmod n$$

- The deciphering function is

$$f_{(n,d)} : \mathbb{Z}_n \to \mathbb{Z}_n, \quad x \mapsto x^d .$$

Problem

An RSA system with 26-letter alphabet and $K_D = (n = 46927, d = 26767)$ has been used to send me the encrypted message

BSSM.

The correspondence

Message units $\longleftrightarrow$ Integers

is of the form

$$YES \longleftrightarrow 24 \cdot 26^2 + 4 \cdot 26 + 18$$

$$= 16346$$

Question: what was the original plaintext in this example?

Soln

Decipher B S S M

↕

$B.26^3 + S.26^2 + S.26 + M$

||

$26^3 + 18.26^2 + 18.26 + 12$

||

30224

Now compute

$(30224)^{28767} \mod 46927$

By computer, this power is

1371

$$1371 = 2.26^2 + 0.26 + 19$$

$$\updownarrow$$

C A T

Public Key Cryptosystems can be used for signing documents.

$$f_D(f_E(\text{word})) = \text{word}.$$

RSA uses Euler's Theorem. This is a special case of

Fermat's Little Theorem

For a prime p and a not divisible by p we have

$$a^{p-1} \equiv 1 \mod p$$

Example $p = 5$

$a = 3$

$a^{p-1} = 3^4 \equiv 1 \pmod 5$

Proof of Fermat's Theorem

Let a, p be as in the theorem.

Consider

$1.a, 2.a, 3.a, \ldots, (p-1).a \pmod p$.

Claim: no two numbers in this list are the same mod p.

(Suppose two numbers, say $i.a, j.a$ were the same.

Then

$i.a \equiv j.a \pmod p$

$i.a - j.a \equiv 0 \pmod p$

$(i-j).a \equiv 0 \mod p$

So p would divide $(i-j).a$.

Since $\gcd(a,p)=1$ we must have p divides $i-j$.

so $i-j \equiv 0 \mod p$

or $i \equiv j \mod p$.)

Now

$(1.a)(2.a)(3.a) \cdots ((p-1).a) \equiv$

$\equiv 1.2.3. \cdots (p-1)\, a^{p-1} \mod p$

$\equiv 1.2.3. \cdots (p-1) \mod p$

So

$(1.2. \cdots p-1) \equiv (1.2. \cdots p-1)\, a^{p-1} \mod p$

So

$1 \equiv a^{p-1} \mod p.$

QED