RSA public key cryptography

(Rivest, Shamir, Adleman 1977)

Suppose

- N letter alphabet (e.g. $N = 26$)
- k-letter plaintext message units
- l-letter ciphertext message units

plaintext message units $\longleftrightarrow$ integers $0 \le i \le N^k$

ciphertext message units $\longleftrightarrow$ integers $0 \le i' \le N^l$

Cryptosystem

- Each user chooses two distinct random prime numbers P, Q (at around 1000 digits each to be safe with modern technology.)

HELLO_WORLD_

H E L L O _ . . . .

HEL LO_ WOR LD_

- Choose an integer e with

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

- Each user computes

$$n = pq$$

and publishes the enciphering key

$$K_E = (n, e)$$

- Each user computes (using the Euclidean algorithm)

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

where $\phi(n) = (p-1)(q-1)$

The deciphering key

$$K_D = (n, d)$$

is kept secret.

The enciphering function is

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

Proposition

$$(x^e)^d = x \mod n$$

- The deciphering function

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

Example of an RSA cryptosystem

26-letter alphabet $A=0, B=1, \ldots, Z=25$

$k=3$: 3-letter plaintext units

$l=4$: 4-letter ciphertext units

I want to send Alice the message

YES

Her published public key is

$$K_E^{Alice} = (n, e)$$

$$= (46927, 39423)$$

$$YES \leftrightarrow 24.26^2 + 4.26 + 18.26^0$$

$$= 16346$$

$$f_{(n,e)}^{Alice}(YES) = 16346^{39423} \mod 46927$$

$$= 21166$$

$21166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26 + 2$

$= BFIC$

I send the encyphered message BFIC.

It is believed that the computation of d necessitates the factorization of n into

$n = pq$.

It is believed that (with current methods) the factorization would take a prohibitively long time.