RSA Public Key Cryptography

(Rivest, Shamir, Adleman 1977)

Suppose

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

Plaintext message units $\longleftrightarrow$ Integers $0 \leq i \leq N^k$

Ciphertext message units $\longleftrightarrow$ Integers $0 \leq i \leq N^l$

Crypto system

- Each user chooses two distinct random prime numbers P, Q (of around 100 digits each to be safe with current technology),

HELLOTHERE

H E L L

HE LL OT HE RE

HEL LOT HIER E--

- 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 is

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

Example of 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

Here published public key is

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

$$= (46927, 39423)$$

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

$$= 16346$$

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

$$\equiv 21166$$

$21166 = 1.26^3 + 5.26^2 + 8.26 + 2$

(5)

$= BFIC$

to send the enciphered message

BFIC.

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

$$n = pq .$$

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