RSA Public Key Cryptosystem

(Rivest, Shamir, Adleman 1977)

Suppose

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

(e.g. $k = 3$

MEET-ME-TONIGHT

MEE, T-M, E-T, ONI, GHT)

- l-letter ciphertext message units

(e.g. $l = 4$

XYABZT13

XYAB, ZT13)

plaintext message units $\longleftrightarrow$ integers in range $0 \leq i \leq N^k$

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

Example of an RSA cryptosystem

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

$k=3$: 3-letter plaintext message units

$t=4$: 4-letter ciphertext " "

I want to send Alice the message

YES

Here public key is found from her webpage to be

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

$$= (46927, 39423)$$

$$YES \leftrightarrow 24 \cdot 26^2 \quad 4 \cdot 26 \quad 18 \cdot 26^0$$

$$= 16346$$

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

$$= 21166$$

The deciphering key

$K_D = (n, d)$

is kept secret.

The enciphering function is

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

Proposition

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

- The deciphering function is

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

Cryptosystem

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

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

where $\varphi(n) = (p-1)(q-1)$.

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

$$= BFIC$$

I send the enciphered message

BFIC.

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

$$n = pq.$$

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