RSA Public Key Cryptosystem

Rivest, Shamir, Adelmann

Suppose:

N letter alphabet (e.g. $N = 26$)

k-letter plaintext message units. (e.g. $k = 3$)

l-letter ciphertext message units. (e.g. $l = 3$)

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

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

The cryptosystem

- Each user chooses two "random" primes P, Q (of around 100 digits each), plus

a random integer

e

with the property that

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

- Each user computes

$$n = pq.$$

and publishes the enciphering key

$$K_E = (n, e).$$

- Each user computes (by the Euclidean Algorithm)

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

From yesterday, we can easily find $\phi(n)$ since

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

The deciphering key is

$$K_D = (n, d)$$

- The enciphering function is

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

Proposition

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

The deciphering function is thus

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

It is believed to be hard to find d starting just with (n, e).

Example

$N = 26$ letter alphabet

$A = 0, B = 1, \cdots, Z = 25$

$k = 3$ 3-letter plain message units

$l = 4$ 4-letter cipher message units

I want to send Alice the message

YES

Her published key is

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

$$= (46927, 39423)$$

YES $\longleftrightarrow$

$24.(26)^2 + 4.26 + 18$

$= 16346$

$= 39423$

$f_{(n,e)}(YES) = 16346$

$\mod 46927$

$= 21166$

$21166 = 1.(26)^3 + 5.(26)^2 + 8.(26) + 2$

$= BFIC$

↖ ciphertext

Remark Frequency analysis is no use with this system. It can only tell us the enciphering key, which we already know.