

RSA Public key cryptosystem

(Rivest, Shamir, Adleman 1977. Cocks 1973)

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

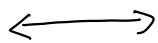
- l -letter ciphertext message units

(e.g. $l=4$)

XYAIBCBA

XYAI, BCBA)

Plaintext
message
units



Integers in the
range
 $1 \leq i \leq N^k$

Ciphertext
message
units



Integers
 $0 \leq i \leq N^l$

Cryptosystem

- Each user chooses two distinct random prime numbers p and q (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 calculates

$$n = pq$$

and publishes the enciphering

$$\text{key } K_E = (n, e)$$

- Each user calculates (using the Euclidean algorithm)

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

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

- The deciphering key $K_D = (n, d)$ is kept secret.

- The enciphering function is

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

- The deciphering function is

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

Yesterday's Lemma

$$(x^e)^d \equiv x \pmod{n}$$

Example of an RSA cryptosystem

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

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

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

h want to send Alice the message:

YES

Alice's public key is found from her web page to be

$$K_E = (n, e) \\ = (46927, 39423)$$

$$\text{YES} \leftrightarrow 24 \cdot 26^2 + 4 \cdot 26 + 18 \cdot 26^0 \\ = 16346$$

$$f_{(n,e)}^{\text{Alice}}(\text{YES}) = 16346^{39423} \pmod{46927} \\ = 21166$$

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

= BFIC

h send Alice the message BFIC.

Remark 1 It is believed that the computation of d necessitates the factorization of n into $n=pq$.

Remark 2 It is believed that (with current technology) that the factorization $n=pq$ would take a prohibitively long time.