

Public Key Encryption Device

MICHAEL TAYLOR

Here we fill in the mathematics behind a public key encryption method described in Chapter 9 of [M]. The ingredients consist of the following.

A. SECRET DATA: p, q (distinct large primes), $\beta \in \mathbb{N}$.

B. PUBLIC DATA: $pq, \alpha \in \mathbb{N}$ (the “key”).

C. MESSAGE: $a \in \{1, \dots, pq\}$.

D. ENCRYPTED MESSAGE: $b = a^\alpha \pmod{pq}$.

E. DECRYPTED MESSAGE: $b^\beta = a \pmod{pq}$.

The secret number β has the crucial property that

$$(1) \quad \alpha\beta = 1 \pmod{(p-1)(q-1)}.$$

The identity of β can be deduced easily from knowledge of p, q , and α , but not so easily from the knowledge merely of pq and α (assuming that it is hard to factor pq).

Here is how a person who knows the public data encrypts a message and sends it to a recipient who knows the secret data. Let us say the secret data is known to Bill. Joe wants to send a message (digitized as a) to Bill. Joe knows the public data. (So do members of the Nosy Snooping Association.) Joe takes the message a and uses the public data to produce the encrypted message b . Then Joe sends the message b to Bill. There is a serious possibility that nosy snoopers will intercept this encrypted message.

Bill uses the secret data to convert b to a , thus decrypting the secret message. To accomplish this decryption, Bill makes use of the secret number β , which is not known to the nosy snoopers (nor to Joe), and, as indicated above, computes $b^\beta \pmod{pq}$.

The mathematical result behind how this works is the following.

Theorem 1. *Let p and q be distinct primes. Assume that α and β are positive integers satisfying (1). Then*

$$(2) \quad a^{\alpha\beta} = a \pmod{pq}, \quad \forall a \in \mathbb{Z}.$$

The key step in the proof is the following.

Lemma 2. *In the setting of Theorem 1,*

$$(3) \quad a^{(p-1)(q-1)} a = a \pmod{pq}.$$

Proof. Note that $\mathbb{Z}/(p)$ is a field and the set of its nonzero elements is a multiplicative group of order $p - 1$. Hence

$$(4) \quad a^{p-1} = 1 \pmod{p}, \quad \text{if } a \not\equiv 0 \pmod{p},$$

so

$$(5) \quad a^{(p-1)(q-1)} = 1 \pmod{p}, \quad \text{if } a \not\equiv 0 \pmod{p}.$$

Thus

$$(6) \quad a^{(p-1)(q-1)} a = a \pmod{p}, \quad \forall a \in \mathbb{Z},$$

since this holds trivially if $a \equiv 0 \pmod{p}$, and otherwise follows from (5). Similarly,

$$(7) \quad a^{(p-1)(q-1)} a = a \pmod{q},$$

and together (6) and (7) imply (3).

One can multiply (3) repeatedly by $a^{(p-1)(q-1)}$, and obtain

$$(8) \quad a^{m(p-1)(q-1)+1} = a \pmod{pq}, \quad \forall a \in \mathbb{Z},$$

whenever m is a positive integer. This yields (2), proving Theorem 1.

Reference

[M] J. MacCormick, 9 Algorithms that Changed the Future, Princeton Univ. Press, Princeton, NJ, 2012.