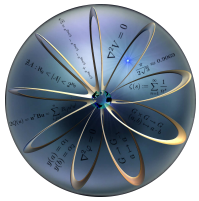

planetmath.org

Math for the people, by the people.

RSA

Canonical name	RSA
Date of creation	2013-03-22 15:14:50
Last modified on	2013-03-22 15:14:50
Owner	aoh45 (5079)
Last modified by	aoh45 (5079)
Numerical id	5
Author	aoh45 (5079)
Entry type	Definition
Classification	msc 94A60
Synonym	RSA cryptosystem

RSA is an example of public key cryptography. It is a widely used system, relying for its security on the difficulty of factoring a large number.

Alice forms her public and private keys as follows:

- Chooses large primes p and q, then form $n = pq$.
- Chooses e coprime with $\phi(n) = (p-1)(q-1)$.
- Publishes (n, e) as her public key.
- Computes private key d such that $de \equiv 1 \mod \phi(n)$.

To encrypt a message M (where $M < n$) the user Bob forms $C = M^e \mod n$.

To decrypt the message, Alice forms $d(C) = C^d \mod n$.

This recovers message M because:

$$\begin{aligned} d(C) &= C^d \mod n \\ &= (M^e + rn)^d \mod n \qquad \text{for some } r \\ &= (M^{(p-1)})^{t(q-1)} M \mod n \qquad \text{for some } t \\ &\equiv (1 + sp)^{t(q-1)} M \mod p \qquad \text{for some } s \\ &\equiv M \mod p \end{aligned}$$

So $d(C) \equiv M \mod p$ and similarly, $d(C) \equiv M \mod q$ so by the Chinese remainder theorem, $d(C) \equiv M \mod n$, and since we know $M < n$ we know that $M = d(C)$.