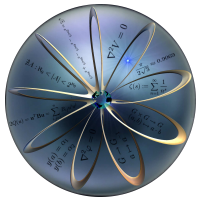

planetmath.org

Math for the people, by the people.

public key cryptography

Canonical name	PublicKeyCryptography
Date of creation	2013-03-22 15:12:38
Last modified on	2013-03-22 15:12:38
Owner	aoh45 (5079)
Last modified by	aoh45 (5079)
Numerical id	4
Author	aoh45 (5079)
Entry type	Definition
Classification	msc 94A60

The basic idea behind public key cryptography, is that a user can publish (for instance on the internet) all the information needed to send them an encypted message, but for this information to be insufficient to decrypt the message in *reasonable time*. In general, this time requirement is taken to that, if the public key has length n (over a particular alphabet), then the message cannot be decrypted in time $\leq p(n)$ for any polynomial p.

The information published to all users is called the *public key*, and the additional information needed to decrypt a message is a users *private key*.

Public key cryptography was first conceived by James Ellis in 1969, and a workable scheme was developed in 1973. This was kept secret however, and it was not until 1978 that two schemes were announced publicly. These were the *Merkle-Hellman* scheme, and the *RSA* scheme.