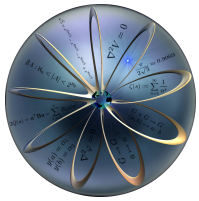

planetmath.org

Math for the people, by the people.

cryptography

Canonical name	Cryptography
Date of creation	2013-03-22 15:49:07
Last modified on	2013-03-22 15:49:07
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	10
Author	CWoo (3771)
Entry type	Definition
Classification	msc 94A60
Synonym	cleartext
Synonym	cyphertext
Synonym	cryptotext
Defines	plaintext
Defines	ciphertext
Defines	message space
Defines	cyphertext space
Defines	key space
Defines	key
Defines	key pair
Defines	encryption function
Defines	decryption function
Defines	cryptosystem
Defines	cryptanalysis

Cryptography is the science of encoding and decoding messages so that they are only understood by intended senders and recipients.

Informally, the basic ingredients in cryptography consist of

1. An alphabet Σ. A word over Σ is called a *plaintext* or *cleartext*. The set $M := \Sigma^*$ of all plaintexts is called the *message space*.

2. An alphabet Δ. A word over Δ is called a *ciphertext* or *cryptotext*. The set $C := \Delta^*$ of all ciphertexts is called the *ciphertext space*.

3. A set K called the key space, such that each $k \in K$, called a *key*, determines functions $e_k : M \to C$ and $d_k : C \to M$ called *encryption function* and *decryption function* respectively. It is generally required that $d_k \circ e_k = 1_M$ (and usually $e_k \circ d_k = 1_C$ so that e_k and d_k are inverses of one another). The pair (e_k, d_k) is usually called a *key pair*.

The triple (M, C, K) is called a *cryptosystem*.

Given a cryptosystem, one generally wants both e_k and d_k to be easily computable, so that encryption by the sender and decryption by the intended receiver can be done effortlessly. For example, if A were to send B an encrypted message, A needs to be able to *easily* encrypt a plaintext u into a ciphertext $v = e_k(u)$. Upon receiving v, the intended receiver B needs to be able to *easily* decrypt v into plaintext $u = d_k(v)$. On the other hand, one also wants the task of recovering the plaintext from the ciphertext very difficult, or intractible, without knowing the decryption functions d_k. For example, if an eavesdropper C ever gets hold of v, he/she will have a very hard time recovering u without knowing d_k, sometimes even in the presence of knowing e_k.

Here, the adjectives "easy", "difficult", "intractible" are measured in terms of the complexity involved in the computations. For example, "easy" could mean that the time involved in the computations depends linearly on the length of the input u (hopefully with a small coefficient), whereas "difficult" could mean the dependence be exponential instead. A function f such that it is easy to compute $f(u)$ given u but very hard to find u given $f(u)$ is usually called a *one-way function*. For example, $f(m, n) = mn$ where m, n are primes, is one-way, or nearly so. It is easy to multiply, but very hard to factor, particularly when both m and n are large.

The study of cryptogrpahy thus can be loosely broken up into two main branches: the construction of a good cryptosystem (meaning that the encryption functions should be one-way, and the decryption functions should

be easy to compute), and the breaking of a ciphertext in some given setting (for example, where the encryption functions are known). The latter of the two branches is also known as *cryptanalysis*.

The mathematics behind cryptography involves a variety of disciplines, of which the main ones are information theory, formal languages, computational complexity, probability theory, and number theory.

Cryptographic methods range from simple additive ciphers to sophisticated public key encryption systems, first introduced by Diffie and Hellman in the mid 1970's.