From Wikipedia entry on **Kerckhoffs's Principle** (date 2011)**:**

1883 Auguste Kerckhoffs in *La Cryptographie Militaire*, six design principles for military ciphers.

1. The system must be practically, if not mathematically, indecipherable;

2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;

3. Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents;

4. It must be applicable to telegraphic correspondence;

5. It must be portable, and its usage and function must not require the concourse of several people;

6. Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

Some are no longer relevant given the ability of computers to perform complex encryption, but his second axiom, now known as Kerckhoffs' Principle, is still critically important.

Principles of Modern Cryptographic cyphers

1. The opponent knows the system being used

2. The opponent has access to any amount of corresponding plaintext and cyphertext.

3. The opponent may have access to the key used in the encrypting transformation.

4. Security is to be achieved by the opponent not being able to construct the decrypting transformation.

Steven Levy's book **crypto** attributes this idea of a split encryption/decryption key to Whit Diffie May 1975.

Trapdoor Ciphers

A map from the message space to the cipher space is called a trapdoor function if the construction of the inverse map is of such computational complexity that it is inaccessible to our present day computational tools.

Note: A trapdoor function may be so today...but maybe not tomorrow.

Possible Trapdoor Functions

EASY	HARD?
Multiplication of integers	Factorization of integers
Raise to a power (mod n)	Discrete log (mod n)
Squaring an integer (mod n)	Taking a square root (mod n)
Sum a set of integers	Searching through sets of numbers to find a subset which gives a specific sum.