Kerckhoffs's Principle

Kerckhoffs's principle (also called **Kerckhoffs's desideratum**, **assumption**, **axiom**, **doctrine** or **law**) of cryptography was stated by the Dutch cryptographer Auguste Kerckhoffs in the 19th century. The principle holds that a cryptosystem should be secure, even if everything about the system, except the key, is public knowledge. This concept is widely embraced by cryptographers, in contrast to security through obscurity, which is not.

Kerckhoffs's principle was phrased by the American mathematician Claude Shannon as "the enemy knows the system",[1] i.e., "one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them". In that form, it is called **Shannon's maxim**.

Security Through Obscurity Considered Dangerous

Hiding security vulnerabilities in algorithms, software, and/or hardware decreases the likelihood they will be repaired and increases the likelihood that they can and will be exploited. Discouraging or outlawing discussion of weaknesses and vulnerabilities is extremely dangerous and deleterious to the security of computer systems, the network, and its citizens. [2]

Open Discussion Encourages Better Security

The long history of cryptography and cryptoanalysis has shown time and time again that open discussion and analysis of algorithms exposes weaknesses not thought of by the original authors, and thereby leads to better and more secure algorithms. As Kerckhoffs noted about cipher systems in 1883, "Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi." (Roughly, "the system must not require secrecy and must be able to be stolen by the enemy without causing trouble.") [2]

[1] https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle

[2] https://www.cs.columbia.edu/~smb/papers/draft-ymbk-obscurity-00.txt

Revision #3
Created 2026-08-28 20:53:16 UTC by Dara
Updated 2026-08-28 21:19:13 UTC by Dara