The information hiding homepage

Kerckhoffs' principles from « La cryptographie militaire »

If your interests include cryptography, you have certainly heard about Kerckhoffs' principles, especially the one stating that the method used to encipher data is known to the opponent, and that security must lie in the choice of key. This does not necessarily implies that the method should be public, but only considered as public during its creation. This was enunciated in the January and February issues of the *Journal des sciences militaires*, 1883.

This journal is still available and, in 1998, I got a copy of Kerckhoffs' article from the British Library. Here is electronic version of both parts:

Auguste Kerckhoffs, '*La cryptographie militaire*', *Journal des sciences militaires*, vol. IX, pp. 5–38, Jan. 1883 [PDF], pp. 161–191, Feb. 1883 [PDF].

Here is an approximate English version of the principles that should apply to a crypto-system:

1. The system must be substantially, if not mathematically, undecipherable;
2. The system must not require secrecy and can be stolen by the enemy without causing trouble;
3. It must be easy to communicate and retain the key without the aid of written notes, it must also be easy to change or modify the key at the discretion of the correspondents;
4. The system ought to be compatible with telegraph communication;
5. The system must be portable, and its use must not require more than one person;
6. Finally, given the circumstances in which such system is applied, it must be easy to use and must neither stress the mind or require the knowledge of a long series of rules.

People who want to find out more about August Kerckhoffs, can refer to:

- Jean-Claude Caraco, Rémi Géraud-Stewart and David Naccache, Kerckhoffs' Legacy, IACR ePrint, May 2020.
- File of "August Kerckhoffs" on Geneanet.

Acknowledgements: Frank Stajano for his scanner and OCR software. Bruno Liénard who helped finishing the corrections on the second part. John Kane and Alejandro López who pointed out few errors in Part II.

Spanish translation by by agencia de traducción.