Classical cryptology was “ruled” by Auguste Kerckhoffs’ (1835 – 1903) principles, which were stated in 1883. Kerckhoffs enumerated six principles for field ciphers.

Desiderata for military cryptography

> It is necessary to distinguish between a system of enciphered writing designed for a temporary exchange of letters among several isolated persons, and a method of cryptography intended to control for an unlimited time the communications of different military leaders. The latter, indeed, may not change their conventions at will or at any given moment. Further, they should never keep on their persons any object or note that would be such as to shed light for the enemy on the meaning of any secret messages that might fall into his hands.
>
> A large number of ingenious arrangements achieve the result desired in the first case. For the second a system must satisfy certain exceptional conditions which I will summarize under the following six headings:
>
> 1. The system must be practically, if not mathematically, indecipherable.
>
> 2. It must not rely upon secrecy, and it must be able to fall into the enemy's hands without disadvantage.
>
> 3. The key should be able to be communicated and stored without the help of written notes, and to be changed or modified at the will of the correspondents.
>
> 4. It must be usable for telegraphic communications.
>
> 5. It must be portable, and its handling and operation must not require the assistance of many people.
>
> 6. Finally, it is necessary, in light of the circumstances in which it must be used, that the system be easy to use, not requiring extreme mental effort nor the knowledge of a large number of rules that must be followed.

These principles appear in Kerckhoffs’ 64-page *La Cryptographie militare* (1883).