Intro stuff

Kerchoff’s principle

> The method must not be required to be secret, and itmust be able to fall into the enemy’s hands without causing inconvenience.

Intuition: all of the security of the system should be concentrated in the **secrecy of the key**, not the secrecy of the algorithms.