Principles -

Kerckhoffs's principle

Only keep hidden the key.
(e.g., make the design public)

Principle of sufficient keys

The number of possible keys must be large.
(e.g., avoid brute force)

Principle of (key) separation

Use different keys for different contexts, compartmentalize.
(e.g., minimise the damage of a leak)

Principle of simplicity

Keep everything simple.
(e.g., unnecessary complexity brings in risks)

Principle of diversity

Use different types of … e.g., cryptographic algorithms.
(e.g., avoid same attacks against all)

Security by default

Keep default configuration as secure as possible.
(e.g., deny access by default)

Principle of minimal trust

Minimise the number of trusted entities, don't trust easily.
(e.g., do not say your secrets to anyone)

Principle of the weakest link

A system cannot be more secure than its weakest component (link).
(e.g., secure all components)

Principle of least privilege

Grant the exact privileges required to perform the job.
(e.g., do not grand less or more privileges)

Security by design

Build in security from start.
(e.g., integrate security in all design and development stages)

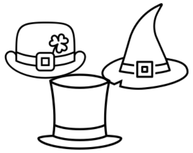
Principle of modularization

Keep things modular.
(e.g., easily change one component with another)

Defence in depth

Use diverse security strategies at different layers.
(e.g., use physical and technological security)

Ethics!



Security through obscurity (?)

Oblivious Transfer, Obfuscation, Covert Channels, … ; Kleptography; Standardisation …

https://pagesonsecurity.blogspot.com/