Security goals

* Confidentiality: keep something secret, data in communication or at rest (cryptography, authentication…)
* Integrity: no corruption or control hijacking, who can write (message, data hashing)
* Availability: system uptime, response time, free storage…
* Privacy: right to be left alone, personal information
* Accountability: login and audit trails (secure timestamping, integrity in logs…)
* Non-repudiation: two parties can’t deny they have interacted (trust a 3rd party and generate evidence)

Security guiding principles

* Secure the weakest link (attacker needs only one flaw)
* Practice defense in depth (use layers of defense)
* Fail securely
* Compartmentalize (separate code into parts)
* Be reluctant to trust
* Principle of least privilege (minimum access and time necessary)
* Keep it simple (to reduce attack surface, tradeoff with usability)
* Promote privacy
* Hiding secrets is hard (hiding details is not enough, attacker can have ways of finding them)
* Use community resources

There are also some attacks described here, come back to check after and see if they were covered.