Cryptographic failures

To understand what falls under the broad category of Cryptographic Failures, it’s important to first understand what cryptography is. Cryptography is a way of securing communication so that sensitive information can only be viewed by authorized parties.

Cryptographic failure refers to situations where the cryptographic mechanisms or practices employed in a system or application fail to provide the intended security protections. This can lead to serious consequences such as unauthorised access to data and data being altered while transmitted. Organizations may suffer financial losses due to cryptographic failures. These losses can include increased costs from legal expenses, regulatory fines, and the loss of business due to reputational damage.

Mitigation Control:

* Use industry-standard encryption algorithms like AES-256, RSA, or ECC.
* Keep encryption libraries and algorithms up to date to mitigate vulnerabilities associated with algorithm weaknesses.
* Conduct regular security audits to identify and replace deprecated cryptographic algorithms.