DATA INTEGRITY IN CRYPTOGRAPHY

Until now, we discussed the use of symmetric and public key schemes to achieve the confidentiality of information. With this chapter, we begin our discussion on different cryptographic techniques designed to provide other security services.

The focus of this chapter is on data integrity and cryptographic tools used to achieve the same.

Threats to Data Integrity

When sensitive information is exchanged, the receiver must have the assurance that the message has come intact from the intended sender and is not modified inadvertently or otherwise. There are two different types of data integrity threats, namely **passive** and **active**.

Passive Threats

This type of threats exists due to accidental changes in data.

- These data errors are likely to occur due to noise in a communication channel. Also, the data may get corrupted while the file is stored on a disk.
- Error-correcting codes and simple checksums like Cyclic Redundancy Checks *CRCs* are used to detect the loss of data integrity. In these techniques, a digest of data is computed mathematically and appended to the data.

Active Threats

In this type of threats, an attacker can manipulate the data with malicious intent.

- At simplest level, if data is without digest, it can be modified without detection. The system can use techniques of appending CRC to data for detecting any active modification.
- At higher level of threat, attacker may modify data and try to derive new digest for modified data from exiting digest. This is possible if the digest is computed using simple mechanisms such as CRC.
- Security mechanism such as Hash functions are used to tackle the active modification threats