Hello everyone! In this video, you will learn about Data Integrity and Message Authentication security concepts and their implementation.

Data integrity requires that the receiver should get the data that is being transmitted without any change. And if any change has been made to the data, it should be detectable, while received on the receiver end.
The cryptography systems that you have studied so far provide secrecy, or confidentiality, but not integrity. However, there are occasions where we may not even need secrecy but instead must have integrity such as a notice issued by the district magistrate to all the schools, regarding holiday on a particular day need to be unchanged but not secret.

Hash Functions play a very important role in ensuring data integrity.
It is a function H that accepts a variable-length block of data as input and produces a fixed-size hash value.
It is a compression function, which means that it takes large blocks of data and outputs smaller size data blocks. A “good” hash function has the property that the results of applying the function to a large set of inputs will produce outputs that are evenly distributed and apparently random. Hash functions are one-way also, therefore it is hard to find the message from the given hash value. In the figure, a Variable-length block of data is given as input to a hashing

function (e.g. SHA-256) and it produces a fixed-size hash value (256 bits)

When two users are communicating through an insecure channel apart from Authentication and Confidentiality users must believe that message is not altered/modified during transmission i.e. the data integrity is ensured. Hash algorithms are used for ensuring Data Integrity. The process can be understood using the given figure.
Message 'M' is encrypted with encryption algorithm 'E' resulting in cipher text 'C'.
Hash function 'H' has been applied on this cipher text 'C' to get fixed size of Hash Code 'HC' also known as digest. After this the Ciphertext and Hash code are sent to receiver through unsecure channel.
Receiver applies Hash function 'H' on 'C`' to get fixed size of Hash Code 'HC' again. This hash code is compared to the received hash code and if found matching, then there is no alteration/modification of message in between and the message is accepted and decrypted using Decryption algorithm. If not found matching, the message is discarded.

If confidentiality is not required, the encryption and decryption steps can be avoided.

Now you know about data integrity very well. It ensures that the message has not been changed. A digest or hash code can be used to check the integrity of a message

Message authentication or data origin authentication , a very important security characteristics , ensures that the message has been received from a legitimate sender, not an adversary.
To ensure the integrity of the message and the data origin authentication i.e. the legitimate sender is the originator of the message, not somebody else—we need to include a secret held by the sender (that is not possessed by the adversary); MAC and Digital signature are two very popular techniques for ensuring message authentication. Let's understand them

When two users are communicating through an insecure channel apart from Confidentiality users must believe that message is not altered/modified during transmission , as well has been sent by the legitimate sender. Message Authentication Code or MAC technique is used for ensuring Data origin authentication. It provides message integrity and message authentication using a combination of a hash function and a secret key.
The process can be understood using the given figure.
Message 'M' is encrypted with encryption algorithm 'E' resulting in cipher text 'C'.
Hash function 'H' has been applied on this cipher text 'C' , along with a secret key possessed by the sender and receiver both ,to get fixed size of Hash Code 'HC' also known as MAC or Message Authentication code. After this the Ciphertext and MAC are sent to receiver through unsecure channel.
Receiver applies Hash function 'H', along with the key on 'C`' to get MAC again. This MAC is compared to the received

MAC and if found matching, then there is no alteration/modification of message, and it has been received from the legitimate sender. The message is accepted and decrypted using Decryption algorithm. If not found matching, the message is discarded.
If confidentiality is not required, the encryption and decryption steps can be avoided.

Another way to provide message integrity and message authentication (and some more security services as we see shortly) is a digital signature.
A MAC uses a secret key to protect the digest; a digital signature uses a pair of private-public keys.

The figure explains the process of signing and verifying a document using digital signature. On sender side a hash to compress the message is generated , which is signed using a signing algorithm(equivalent to the encryption process of public key cryptography) and sender's private key.
the signature is appended to the message and sent to the receiver.
on receiver side, the signature is verified using verification algorithm (equivalent to the decryption process of public key cryptography) and the public key of the sender.
The hash at receiver side is recalculated using the received message and compared with the received hash during the verification process. If both hashes match, then the message is authenticated, otherwise, it is discarded.

Here are some differences between digital signatures and pen-based physical signatures known as manual signatures.

The manual signatures are done inside the document to be authenticated while the digital signatures are appended to the document after creation.

The manual signatures are verified by carefully watching, while digital signatures are verified using mathematical computations.

The same manual signature can be used with multiple documents, while one digital signature cannot be used with multiple documents. It is unique for each document.

Manual signatures can be duplicated, but digital signatures cannot be duplicated.

To learn more about Data Integrity and Authentication, follow the books given here.

Thank You…