Hello everyone! In this video you will understand cryptography and the security services offered by it.

Data have always been an asset to us and need to be secure from attacks. In the past, when data were stored as physical files, security was provided through physical measures. With advancements in technology and the rapid digitalization of data, a huge amount of digital data is stored in databases, servers, the cloud, and other storage devices. Confidential data requires security while storing as well as in transit through insecure communication channels.

To secure the data in any form necessary techniques are needed and Cryptography is considered the best method for this.

Cryptography is about the design and analysis of mathematical techniques that enable secure communications in the presence of malicious adversaries or attackers.

In Figure 1, A(Alice) and B(Bob) are using an unprotected channel to communicate. All conversations are presumably held in the presence of enemy E (Eve), whose goal is to undermine any security services being offered to A and B.

Copyrighted Content

Let's understand the security goals of confidentiality, Integrity, and authentication related to data or information during communication.

Confidentiality means keeping data secret from all but those authorized to see it—messages sent by sender to receiver should not be readable by attackers. Here, in the figure, the sender encrypts the plaintext using a key generating a ciphertext. The ciphertext is send through an insecure communication channel. The receiver deciphers the ciphertext to plaintext using the correct key. While the attacker may get the ciphertext but, as he/she does not have the correct key, he/she cannot get the plaintext.

Data integrity ensures that data has not been altered by unauthorized means i.e. receiver should be able to detect when data sent by sender has been modified by attacker. In the figure, when receiver gets a data from the sender, the receiver should be able to determine whether the received data is altered or unaltered.

another security goal Data origin authentication validates the source of data—receiver should be able to verify that data purportedly sent by sender indeed originated with the authentic sender. In the figure, when receiver gets the data from the sender, the receiver should be able to determine that data received came from the authentic sender.

Copyrighted Content

Let's understand how Cryptography helps us in achieving these security goals. Cryptography provides five key security services Confidentiality, Integrity, Authentication, Non-repudiation and Availability

Confidentiality protects plain data from unauthorized access. Confidentiality is provided by converting the plaintext into cipher text through encryption such that only the intended user with the correct key can have access to the plaintext while at rest or in transit.

Integrity is used to define the completeness of the data. Hash value in cryptography helps in providing integrity of the data by making sure that the data is not modified from what was actually stored or what was actually transmitted. A hash value is a fixed length message digest generated from a variable length message. The hash value is sent along with the cipher message to check the integrity of the message sent by the sender.

Authenticity is used to claim that the sender is indeed an authentic sender and not a hoax. Authenticity is provided through digital signature that is created using the private key of the sender.

Non-repudiation helps in protecting against refusal by either the sender or the receiver. Non-repudiation helps in proving the origin of data sent by the sender or proof of delivery to the receiver if denied.

Data has to be made available only to the authorized entity for any operation such as reading, writing or any update.

Copyrighted Content

Cryptography can be understood using the given cycle of plaintext, encryption, cipher text, and decryption. Let's understand these terms one by one.
Plain text is the information being transmitted in its raw form.

Encryption is the process of converting plain text into unintelligible data called cipher text, especially to prevent unauthorized access.
Decryption is generally the reverse process of encryption. It is the process of decoding the cipher text into plain text.
In the figure an image data(plain text) is encrypted into cipher text and then decrypted using cryptography.

Thank you…

Copyrighted Content