CSS2C08

COMPUTER NETWORKS

MODULE 5
Security in Networks

1. **Principles of cryptography**
2. Authentication
3. Integrity
4. Key distribution and certification
5. Firewalls
6. Attacks and counter measures

Principles of cryptography

1. Message Confidentiality
2. Message Integrity
3. Message Authentication
4. Message Nonrepudiation
5. Entity Authentication

1. Message Confidentiality

- Message confidentiality or privacy means that the sender and the receiver expect confidentiality.
- The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage.
- When a customer communicates with her bank, she expects that the communication is totally confidential.

2. Message Integrity

- Message integrity means that the data must arrive at the receiver exactly as they were sent.
- There must be no changes during the transmission, neither accidentally nor maliciously.
- As more and more monetary exchanges occur over the Internet, integrity is crucial.
- For example, it would be harmful if a request for transferring $100 changed to a request for $10,000 or $100,000.
- The integrity of the message must be preserved in a secure communication.

3. Message Authentication

- Message authentication is a service beyond message integrity.
- In message authentication the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.

4. Message Nonrepudiation

- Message nonrepudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send.
- The burden of proof falls on the receiver.
- For example, when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.

5. Entity Authentication

- In entity authentication (or user identification) the entity or user is verified prior to access to the system resources (files, for example).
- For example, a student who needs to access her university resources needs to be authenticated during the logging process. This is to protect the interests of the university and the student.