Thapar Institute of Engineering & Technology
(Deemed to be University)
Bhadson Road, Patiala, Punjab, Pin-147004
Contact No. : +91-175-2393201
Email : info@thapar.edu

THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)

Course: Computer and Communication Networks

Topic: Network Security

Faculty Name

Dr. Amanpreet Kaur

Assistant Professor

Department of Electronics and Communication Engineering,

Thapar Institute of Engineering and Technology, Patiala.

www.thapar.edu

Outline of the Lecture

❑**Network Security**

❑**Security Services**

- ***Message***

✓*Message confidentiality*

✓*Message integrity*

✓*Message authentication*

✓*Nonrepudiation*

- ***Entity***

✓*Entity authentication*

Network Security

- *Network security is the process of taking preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction or improper disclosure.*

❑How can we ensure network security?

- must ensure that the passwords are Strong and Complex everywhere-

❑Why is security so important?

- The organisation's ability to function without any hindrance
- Enabling the safe operation of applications implemented on the organisation's IT systems
- Protecting the data the organisation collects and its uses

❑What are the different types of Network Security?

➢***Access Control :*** block unauthorized users and devices.

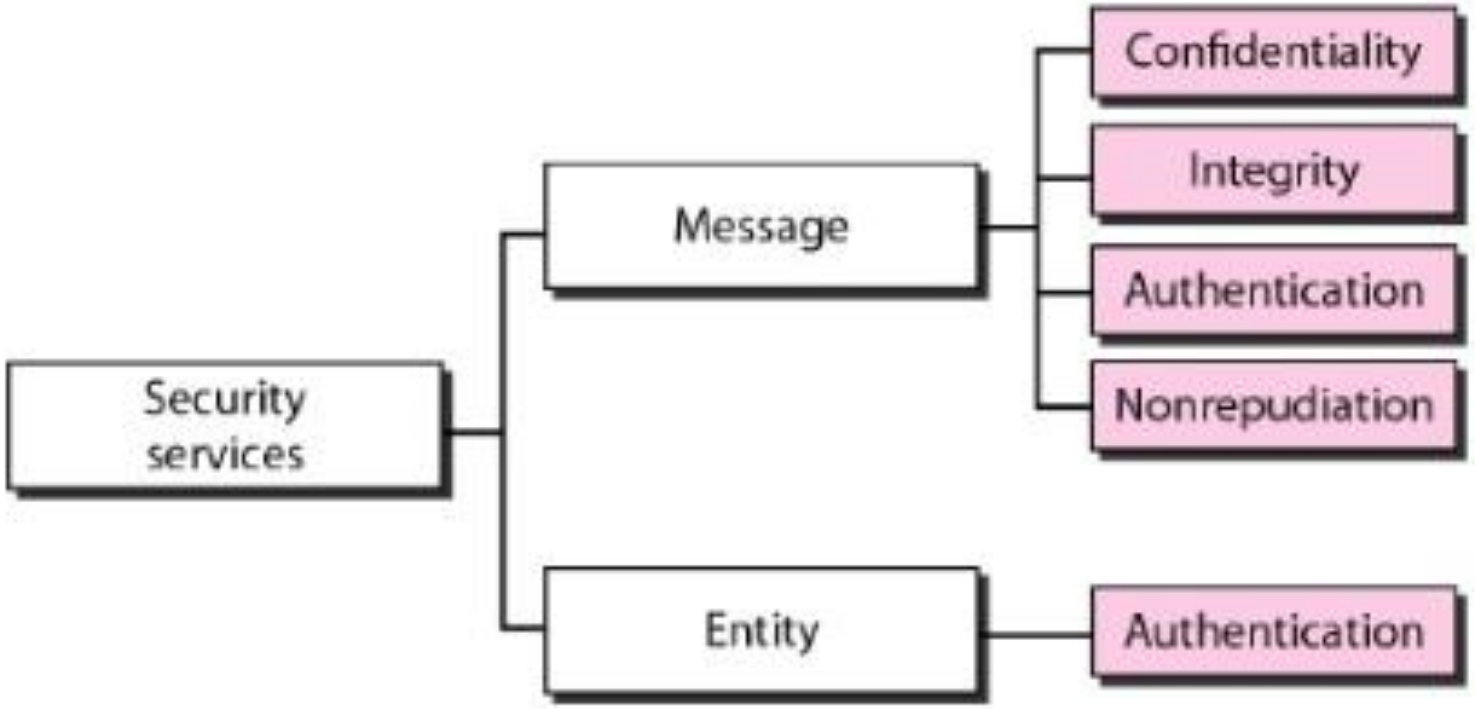
https://www.tutorialspoint.com/ https://www.edureka.co/

Cont…

- ***Application Security****:* hardware, software, and processes that can be used to track and lock down application vulnerabilities.
- ***Firewalls:*** use a set of defined rules to allow or block traffic.
- ***Virtual Private Networks(VPN):*** A virtual private network encrypts the connection from an endpoint to a network.
- ***Behavioral Analytics:*** Behavioral analytics tools automatically identify activities that deviate from the norm.
- ***Wireless Security:*** Cybercriminals are increasingly targeting mobile devices and apps. So, need to control which devices can access your network
- ***Intrusion Prevention System:*** These systems scan network traffic to identify and block attacks

https://www.tutorialspoint.com/ https://www.edureka.co/

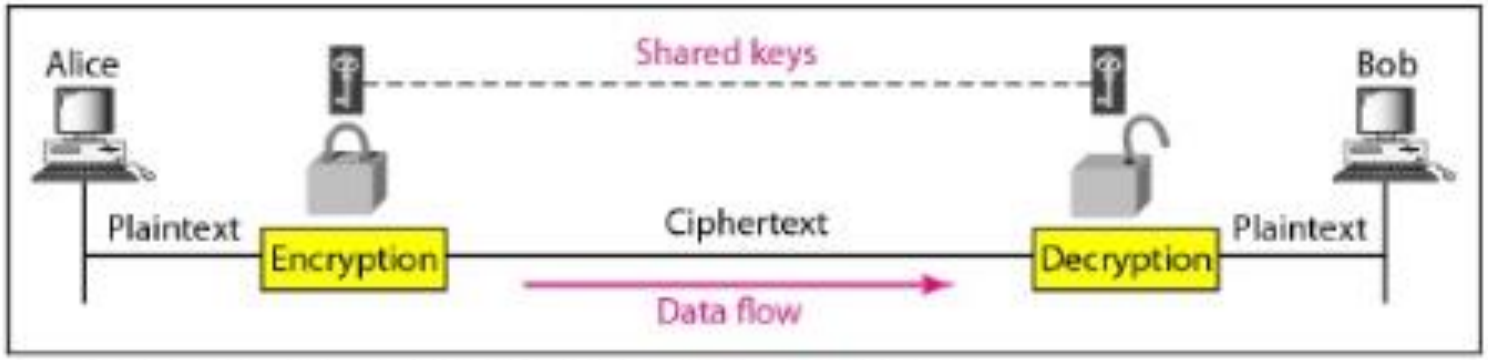
Security Services



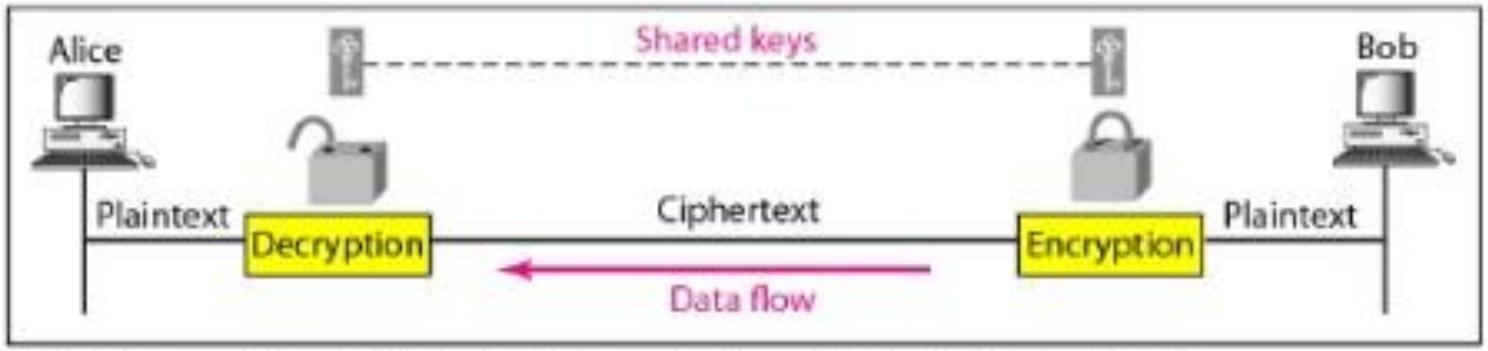
Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking,

Message confidentiality

Confidentiality with Symmetric-Key Cryptography



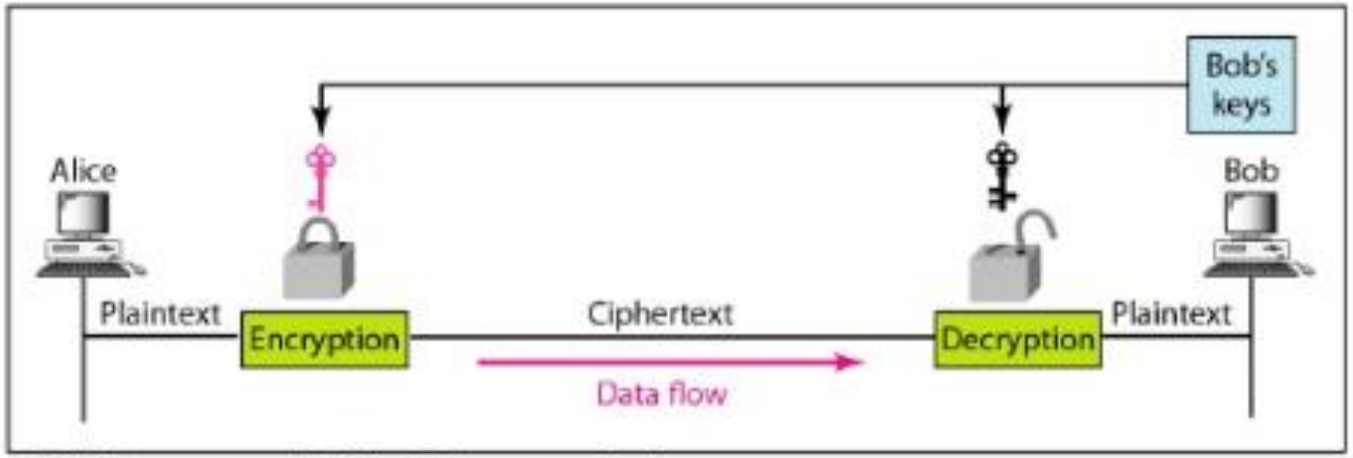
a. A shared secret key can be used in Alice-Bob communication



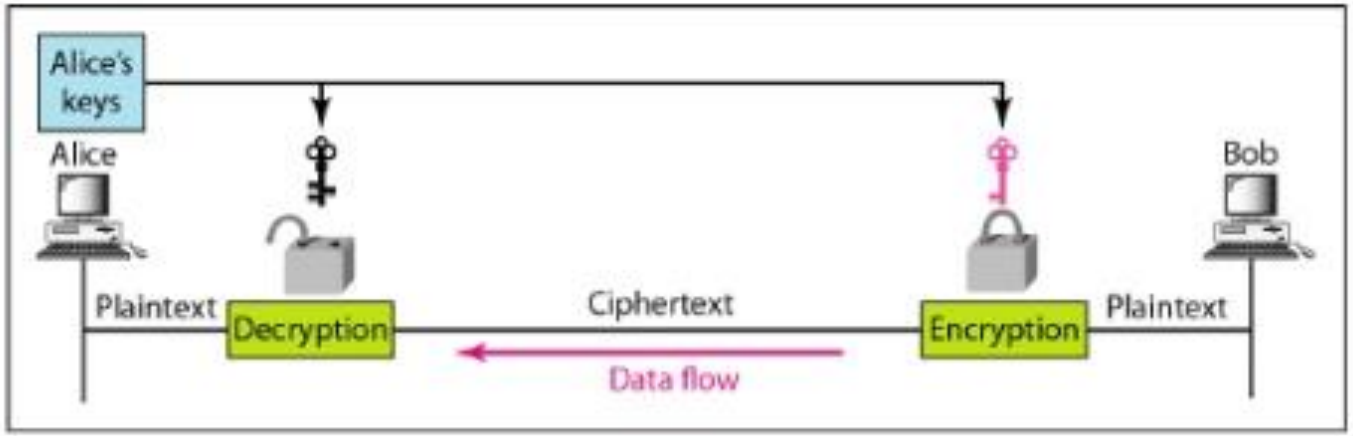
b. A different shared secret key is recommended in Bob-Alice communication

Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking,

- Confidentiality with Asymmetric-Key Cryptography



a. Bob's keys are used in Alice-Bob communication

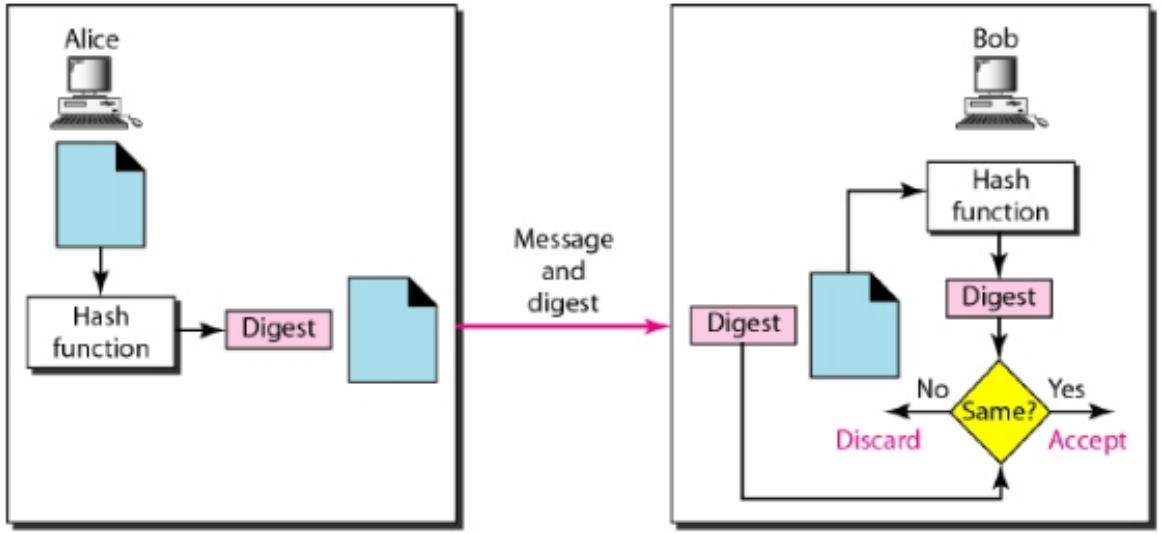


b. Alice's keys are used in Bob-Alice communication

Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking,

Message integrity

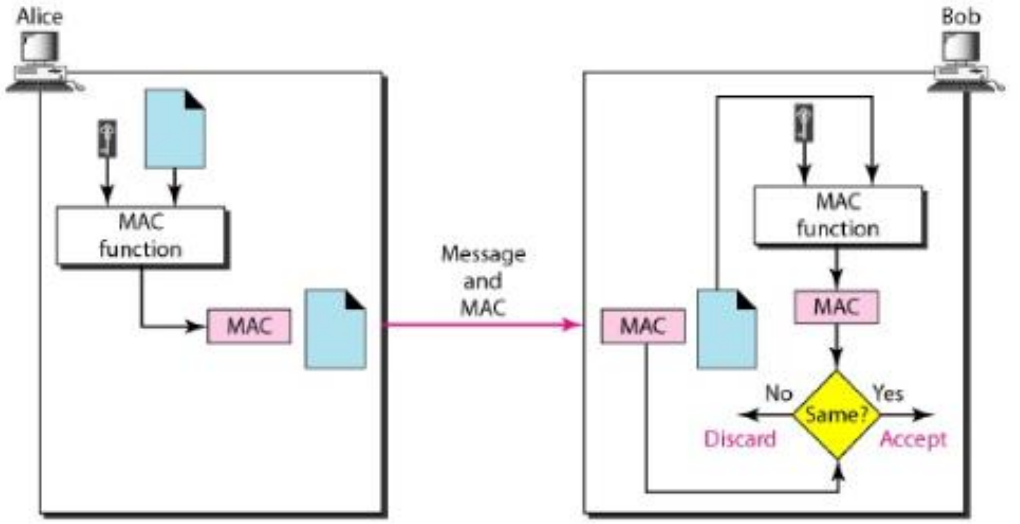
- *Document and Fingerprint*
- *Message and Message Digest*
- *Creating and Checking the Digest*



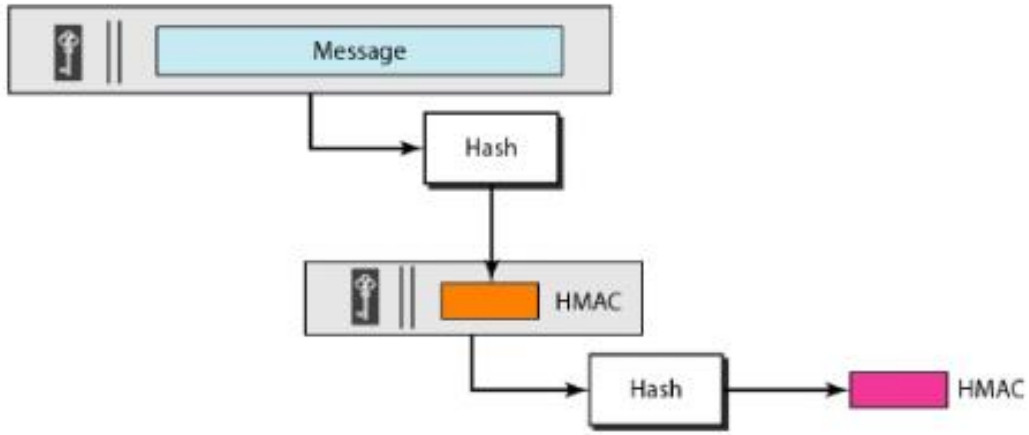
Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking,

Message authentication

- Message Authentication Code (MAC)



- *HMAC*



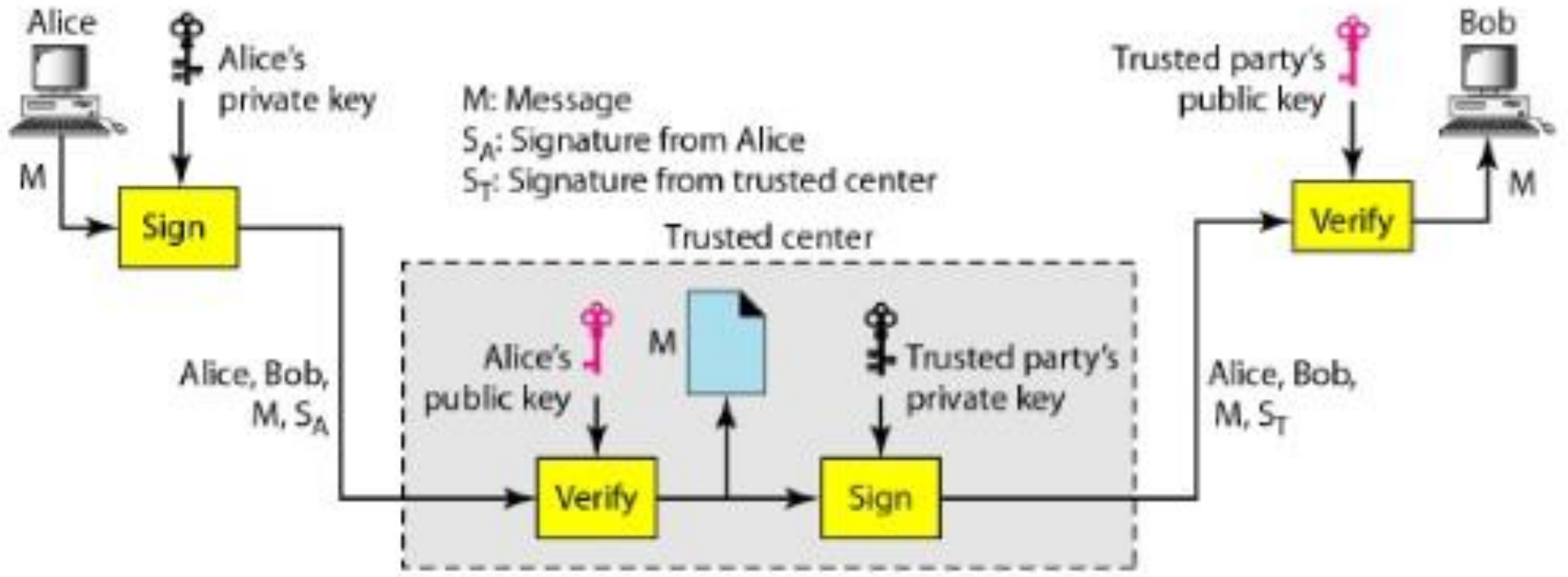
Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking,

Digital signature

- *Inclusion*
- *Verification Method*
- *Relationship*
- *Duplicity*

Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking,

Nonrepudiation



Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking,

Entity authentication

Entity authentication is a technique designed to let one party prove the identity of another party. An *entity* can be a person, a process, a client, or a server.

- Passwords: A password is used when a user needs to access a system to use the system's resources.

✓*Fixed Password*

✓*One-Time Password*

- Challenge-Response : In challenge-response authentication, the claimant proves that she knows a secret without revealing it.

✓*Using a Symmetric-Key Cipher*

✓*Using Keyed-Hash Functions*

✓*Using an Asymmetric-Key Cipher*

✓*Using Digital Signature*

Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking,

Thank You