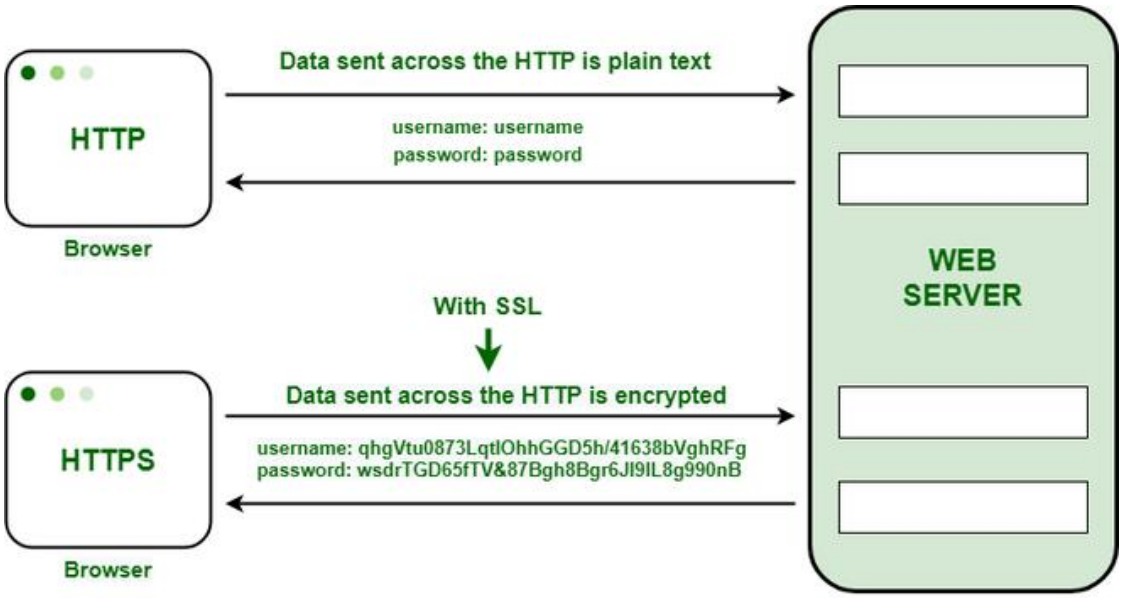
Network security protocols

Network security protocols are essential for protecting data as it travels across networks. Here are some common network security protocols with simple examples to help illustrate their functions:

1. SSL/TLS (Secure Sockets Layer/Transport Layer Security)

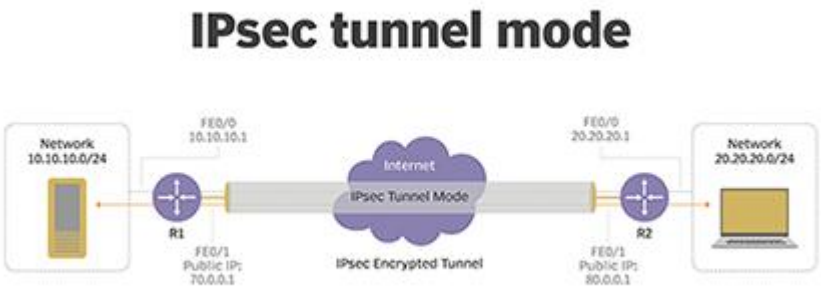
Purpose: Encrypts data transmitted over the internet to ensure privacy and data integrity.



Example: When you access a secure website (e.g., one that starts with https://), SSL/TLS encrypts the connection between your browser and the server, preventing eavesdroppers from reading your data.

2. IPsec (Internet Protocol Security)

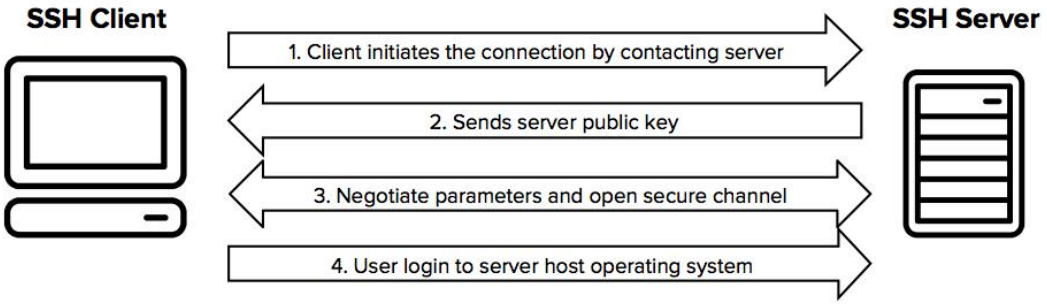
Purpose: Secures IP communications by authenticating and encrypting each IP packet in a communication session.



Example: When a company uses a Virtual Private Network (VPN) to allow remote employees to securely access the company's internal network, IPsec can be used to encrypt the data transmitted over the internet.

3. SSH (Secure Shell)

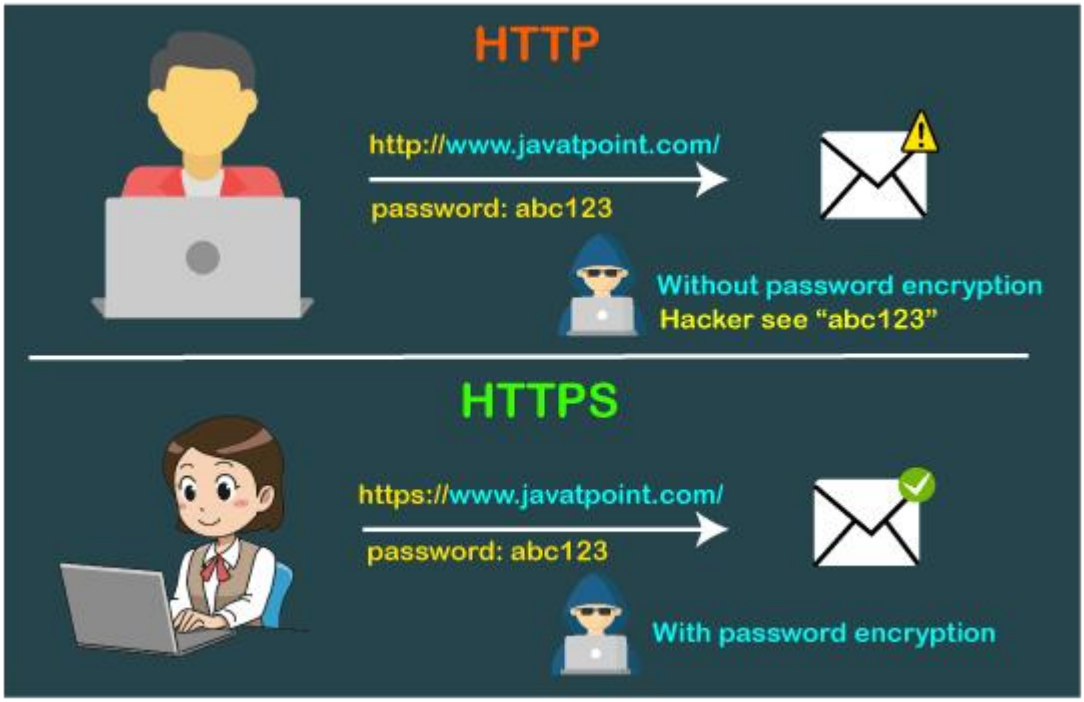
Purpose: Provides a secure channel over an unsecured network for managing servers and network devices.



Example: A system administrator can use SSH to remotely log into a server and execute commands securely without the risk of their password being intercepted.

3. HTTPS (HyperText Transfer Protocol Secure)

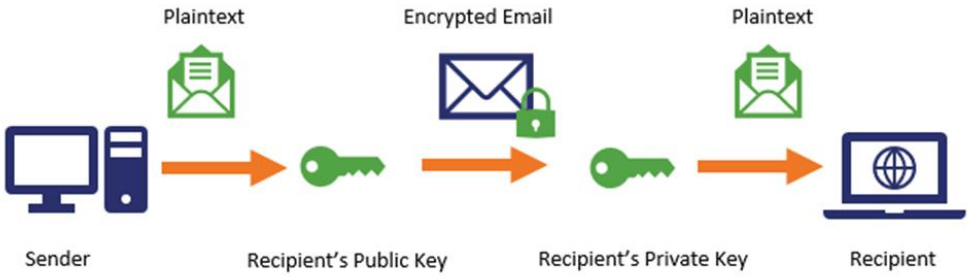
Purpose: An extension of HTTP that uses SSL/TLS to provide secure communication over a computer network.



Example: When shopping online, HTTPS ensures that your credit card information is securely transmitted to the retailer's server.

4. S/MIME (Secure/Multipurpose Internet Mail Extensions)

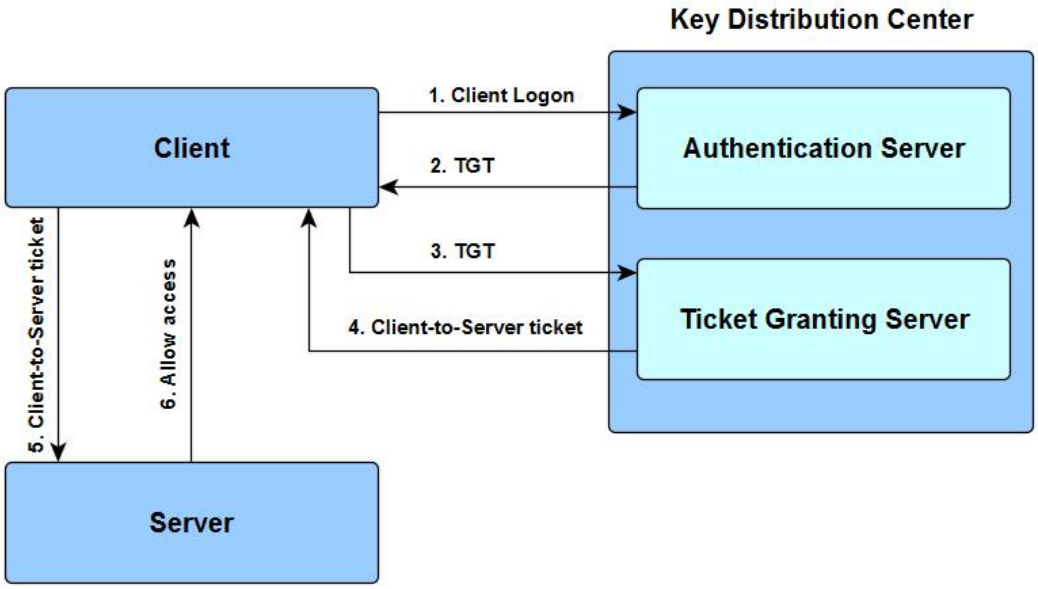
Purpose: Used to encrypt and digitally sign email messages.



Example: When sending a sensitive document via email, using S/MIME ensures that only the intended recipient can read it and verifies that the email was sent by you.

5. Kerberos

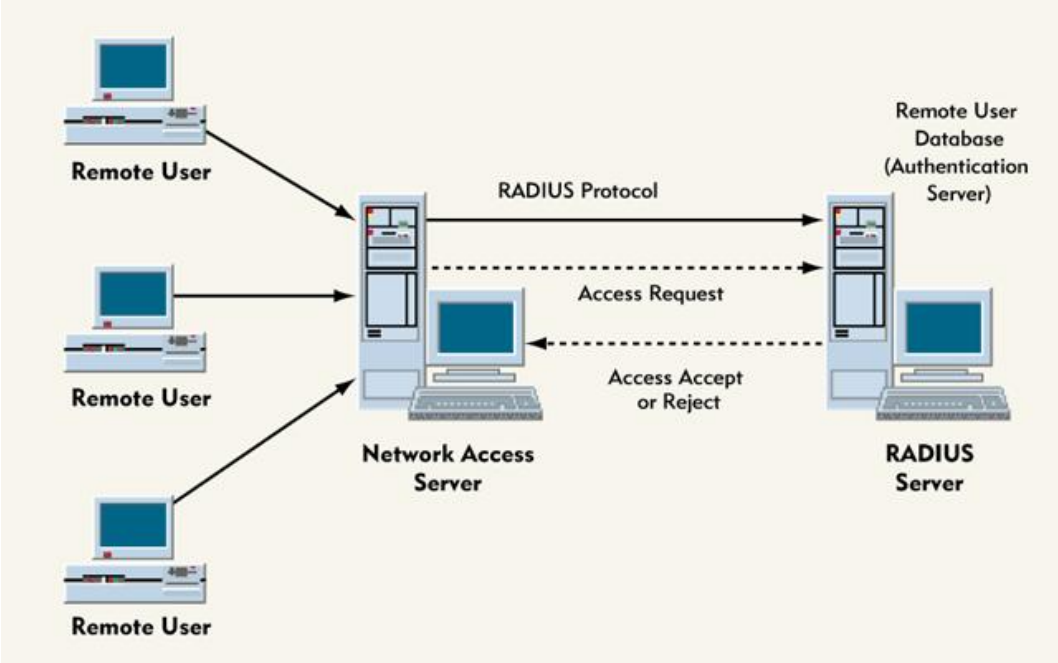
Purpose: A network authentication protocol designed to provide strong authentication for client/server applications.



Example: In a corporate network, Kerberos can be used to authenticate users accessing various services (like file shares or email) without requiring them to log in repeatedly.

6. RADIUS (Remote Authentication Dial-In User Service)

Purpose: Provides centralized authentication, authorization, and accounting for users who connect and use a network service.



Example: When you connect to a Wi-Fi network at a university, RADIUS can verify your credentials (like your student ID) before granting access to the internet.