How HTTPS works?  
  
  
HTTPS is a secure version of the HTTP protocol used for communication on the World Wide Web. It ensures the confidentiality and integrity of data exchanged between a web browser and a web server. Here's how HTTPS works:  
  
1. SSL/TLS Handshake:  
  When a user's web browser connects to a website that uses HTTPS, the browser initiates a secure connection by requesting the server's SSL/TLS certificate. This certificate contains the server's public key, and it is signed by a trusted Certificate Authority (CA).  
  
2. Certificate Validation:  
  The browser checks the certificate's authenticity by verifying that it's signed by a trusted CA and has not expired. If the certificate is valid, the browser proceeds with the connection. If not, it may display a warning to the user.  
  
3. Key Exchange:  
  The browser generates a random symmetric key (session key), which will be used to encrypt and decrypt data during the session. The browser then encrypts this session key with the server's public key obtained from the certificate and sends it to the server.  
  
4. Encrypted Data Exchange:  
  Once the server receives the session key, both the browser and server use it to encrypt and decrypt data sent between them. This ensures that any data transmitted between the two parties is protected from eavesdropping and tampering.  
  
5. Secure Communication:  
  From this point onward, all data exchanged between the browser and server, including web pages, images, forms, and any other content, is transmitted securely. Even if intercepted, it would be extremely difficult for an attacker to decipher the information without the session key.  
  
6. Ongoing Session:  
  The secure session remains active for the duration of the user's interaction with the website. The session key is used to encrypt and decrypt data, and new keys are often generated periodically to enhance security.  
  
HTTPS provides the following security benefits:  
  
1. Data Confidentiality: It prevents eavesdropping by encrypting data, making it unreadable to anyone intercepting the traffic.  
  
2. Data Integrity: It ensures that the data exchanged between the client and server is not altered during transmission.  
  
3. Authentication: It verifies the identity of the server, which helps users trust the website they are interacting with.  
  
HTTPS is crucial for protecting sensitive information, such as login credentials, credit card details, and personal data, during online transactions and other web activities. It has become the standard for secure communication on the internet and is widely used to safeguard online interactions.

Activate to view larger image,

