SSL/TLS

HTTPS is HTTP with an additional SSL/TLS layer for encryption
it helps to maintain privacy and data integrity
the function of a SSL layer is to verify the server (or client)
    and ensure that only the designated server can read what the client sends
    and only the client can read what the designated server sends

goals of SSL/TLS
    cryptographic security
        to maintain secure connection between two parties
    interoperability
        developers should be able to develop apps utilizing TLS without knowledge of other secure code
    extensibility
        whenever needed, new public-key encryption methods should be able to be implemented
    relative efficiency
        session caching schemes are used to reduce the number of connection establishments

structure and functions of SSL/TLS
    SSL/TLS is made up of two main protocols
        TLS Handshake Protocol
        TLS Record Protocol

    TLS Handshake Protocol
        helps ensure that the client is communicating with the right server
        its goal is to help both parties agree on a cryptosystem, including the algorithms
        it also performs necessary key exchanges

        process
            hello
                ClientHello (contains all needed information) is sent to the server
                the server responds with ServerHello
            certificate exchange
                the server proves an identity by providing a SSL certificate
                the client can do this too
            key exchange
                both parties exchange the key for symmetric cryptography

        authenticates the identity using public-key cryptography (like RSA)
            authentication is optional; however, it's usually required for at least one of the peers
        ensures that the negotiation of the shared secret is secure (prevents eavesdropping)
        ensures that the negotiation is reliable
        prevents man-in-the-middle attacks (attacks are detected)

    TLS Record Protocol
        helps ensure the data is securely delivered while its integrity is preserved

        process for transmission
            takes data to be transmitted
            fragments the message into manageable blocks
            compresses the data (optional)
            applies MAC (message authentication code)

encrypts the data
transmits the ciphertext

process for receipt

received data is decrypted
data is verified (MAC)
data is reassembled
data is delivered to high-level clients (i.e., applications)

ensures that the connection is private and reliable
symmetric cryptography is used to exchange messages
message transport includes integrity checking using MAC