1

1. What is the primary function of the Secure Socket Layer (SSL) and Transport Layer Security (TLS)?

A) To encrypt data stored on web servers

B) To provide a secure channel between two machines communicating over the internet

C) To authenticate users logging into websites

D) To compress data before transmission over the internet

2

2. Which of the following is NOT a parameter associated with the SSL connection state?

A) Server and client random values

B) Session identifier

C) Server write MAC secret

D) Initialization vector

3

3. What is the purpose of the SSL Handshake Protocol?

A) To fragment, compress, and encrypt data before transmission

B) To decrypt, verify, and decompress data after reception

C) To authenticate communicating parties, negotiate encryption algorithms, and establish cryptographic keys

D) To define the structure of SSL messages and their fields

4

4. The Change Cipher Spec Protocol in SSL is primarily used for:

A) Negotiating the initial encryption algorithms

B) Notifying about changes in cipher parameters

C) Transmitting the server's certificate

D) Verifying the client's certificate

5

5. Which of the following is a part of the four phases of the SSL Handshake Protocol?

A) Generating MAC

B) Establish Security Capabilities

C) SSL Record Protocol

D) Alert Protocol