EIE424 Distributed Systems and Network Programming – Part II

Quiz: Web Services Security 1

A. Which of the following is NOT the reason why we need extra measures other than HTTPS/SSL to allow security in Web services?

1. We need end-to-end security rather than point-to-point security in Web services.
2. HTTPS/SSL may incur higher computational complexity due to the unnecessary encryption of unimportant information.
3. HTTPS/SSL can be easily attacked by imposter hence extra measures are required.
4. Web services may involve many parties jointly providing the services. There is a need to ensure that every party cannot repudiate the messages they send.

B. What is the major problem of symmetric encryption?

1. The computational complexity of symmetric encryption algorithm is very high.
2. It is difficult to ensure the key can be securely distributed to the receiver.
3. The same algorithm has to be used for both encryption and decryption.
4. Receiver needs a different key to decrypt the encrypted message.

C. Which of the following is NOT correct about the digital envelope approach in enabling secure transmission of information on the Web?

1. The digital envelope approach allows secure distribution of symmetric key to the receiver.
2. Both symmetric and asymmetric encryption approaches are used in the digital envelope approach.
3. Symmetric key is generated by the sender and the asymmetric keys are generated by the receiver.
4. The digital envelope approach allows the sender to prove that he is the originator of the message.