Isfahan University of Technology
Network Security
Dr. Manshaei
Homework 3: Module 4&5 (PKI/TLS)
Deadline: Monday 20th **Azar, at** 23 : 59

We only accept the homework **delivered via Yekta (yekta.iut.ac.ir), before the deadline**. If you have any questions or concerns about this homework, feel free to contact Mr. Sepehr Shirani via Telegram: @*sepovsky* (Preferred) or email: sepishiran@gmail.com.

Theoretical Questions

Q1: Consider the following threats to Web security and describe how each is countered by a particular feature of SSL.

- **Brute-Force Cryptanalytic Attack:** An exhaustive search of the key space for a conventional encryption algorithm.
- **Known Plaintext Dictionary Attack:** Many messages will contain predictable plaintext, such as the HTTP GET command. An attacker constructs a dictionary containing every possible encryption of the known plaintext message. When an encrypted message is intercepted, the attacker takes the portion containing the encrypted known plaintext and looks up the ciphertext in the dictionary. The ciphertext should match against an entry that was encrypted with the same secret key. If there are several matches, each of these can be tried against the full ciphertext to determine the right one. This attack is especially effective against small key sizes (e.g., 40-bit keys).
- **Replay Attack:** Earlier SSL handshake messages are replayed.
- **Man-in-the-Middle Attack:** An attacker interposes during key exchange, acting as the client to the server and as the server to the client.
- **Password Sniffing:** Passwords in HTTP or other application traffic are eavesdropped.
- **IP Spoofing:** Uses forged IP addresses to fool a host into accepting bogus data
- **IP Hijacking:** An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts.
- **SYN Flooding:** An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacked TCP module typically leaves the "half-open connection" around for a few minutes. Repeated SYN messages can clog the TCP module.

Q2: Is it possible in SSL for the receiver to reorder SSL record blocks that arrive out of order? If so, explain how it can be done. If not, why not?

Q3: Figure 1 shows a simplified version of the (simple) TLS handshake between a client and a server, presented as a message sequence diagram. In the diagram, we assume that:

- Cert(Pk, CertA) denotes a certificate issued by a certificate authority CertA, containing the public key Pk.
- The dashed arrows at the end of the protocols denote encrypted communication.
- The client and server finished messages at the end of the protocol include the name of the corresponding entity and a hash of all random strings in the protocol run.

1. Describe the guarantees that each of the involved parties (client and server) have after the execution of the protocol. For each of the guarantees argue (informally) why it should hold, i.e., what are the necessary prerequisites for the protocol to achieve the corresponding guarantee?
2. Give an example of an application scenario in which it makes sense to use this form of TLS handshake.

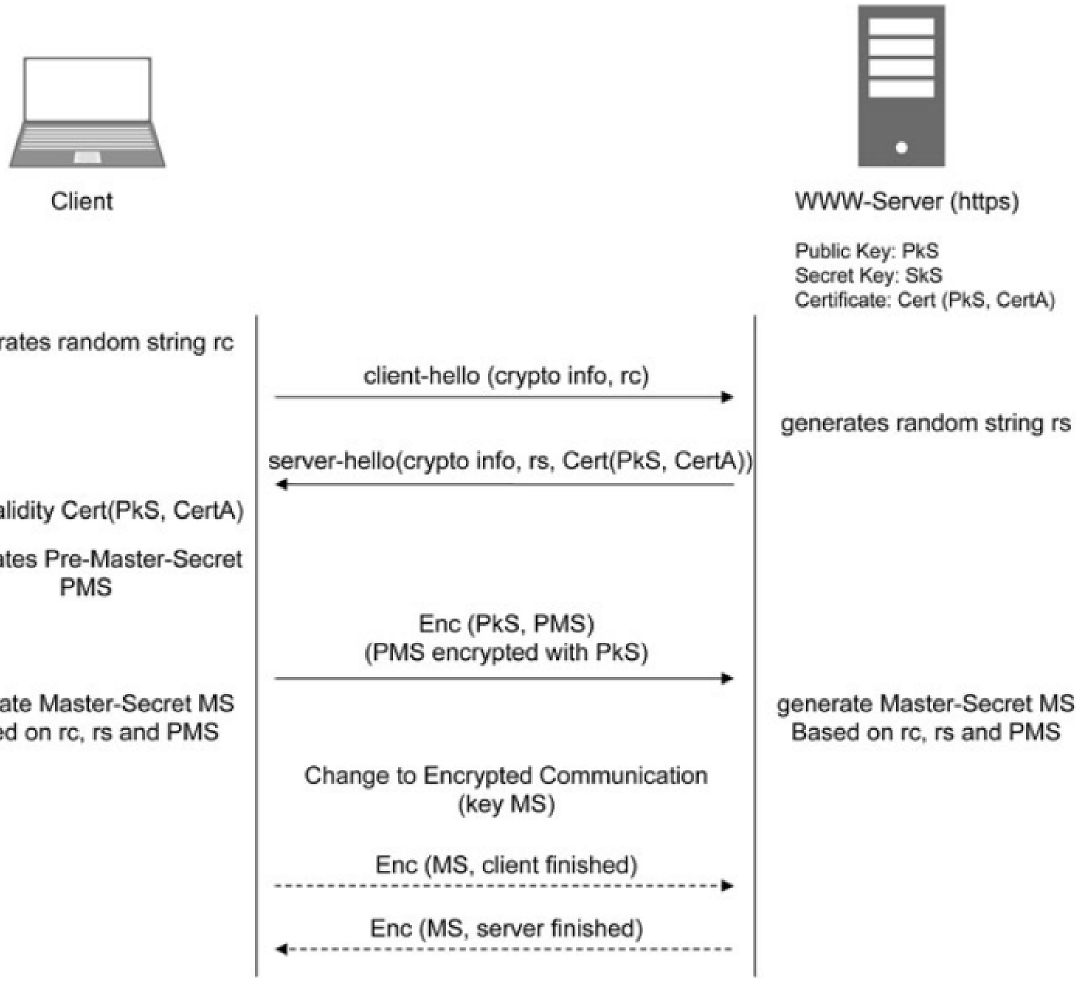
Client
WWW-Server (https)
Public Key: PkS
Secret Key: SkS
Certificate: Cert (PkS, CertA)
generates random string rc
client-hello (crypto info, rc)
generates random string rs
server-hello(crypto info, rs, Cert(PkS, CertA))
check validity Cert(PkS, CertA)
generates Pre-Master-Secret PMS
Enc (PkS, PMS)
(PMS encrypted with PkS)
generate Master-Secret MS based on rc, rs and PMS
generate Master-Secret MS Based on rc, rs and PMS
Change to Encrypted Communication (key MS)
Enc (MS, client finished)
Enc (MS, server finished)

Figure 1: Simplified TLS handshake

Q4: Figure 2 and Figure 3 illustrate two key distribution schemes of a local area network vendor. Compare these two schemes! What are the merits and demerits?

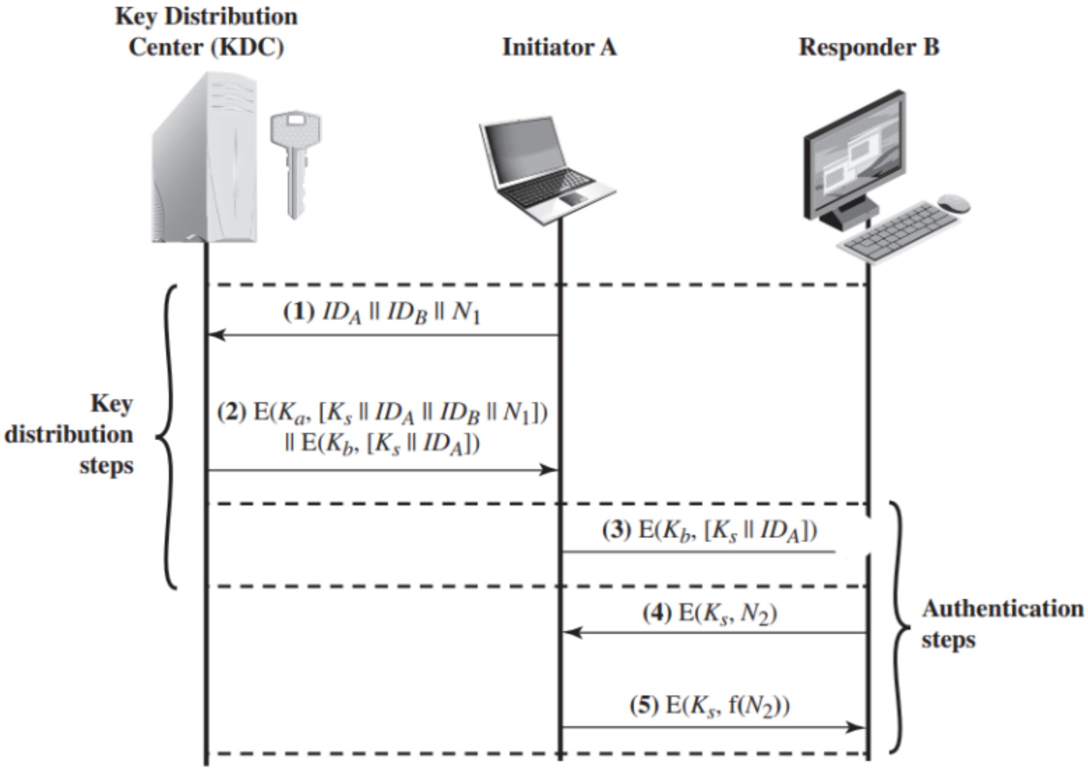
Key Distribution Center (KDC)
Initiator A
Responder B
Key distribution steps
(1) $ID_A \| ID_B \| N_1$
(2) $E(K_a, [K_s \| ID_A \| ID_B \| N_1]) \| E(K_b, [K_s \| ID_A])$
(3) $E(K_b, [K_s \| ID_A])$
(4) $E(K_s, N_2)$
(5) $E(K_s, f(N_2))$
Authentication steps

Figure 2: key distribution center A

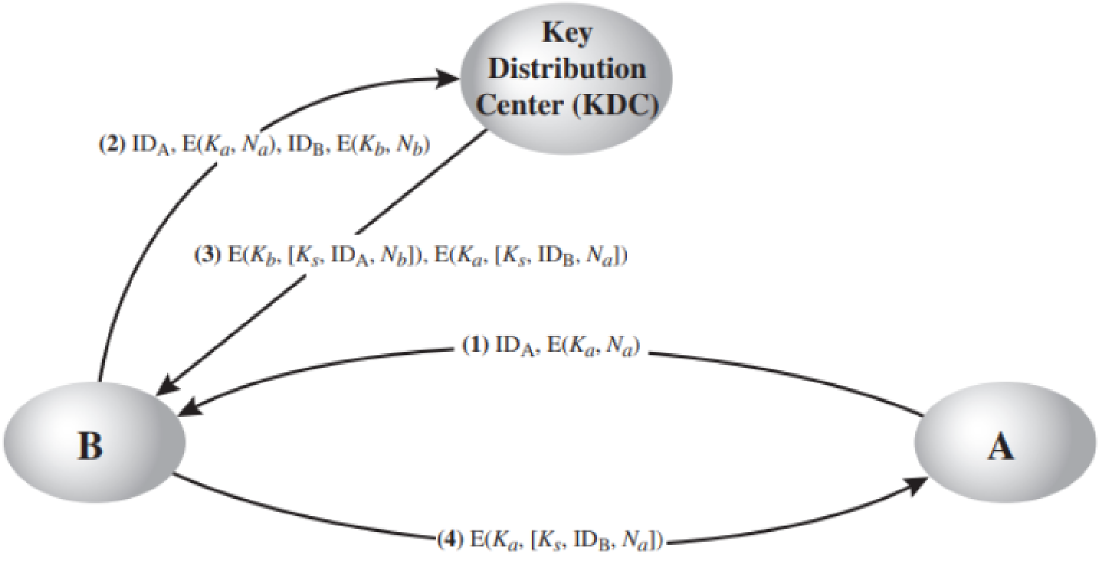
Key Distribution Center (KDC)
(2) $ID_A, E(K_a, N_a), ID_B, E(K_b, N_b)$
(3) $E(K_b, [K_s, ID_A, N_b]), E(K_a, [K_s, ID_B, N_a])$
(1) $ID_A, E(K_a, N_a)$
B
A
(4) $E(K_a, [K_s, ID_B, N_a])$

Figure 3: key distribution center B

Q5: Why must a CRL be reissued periodically, even when no new certificates have been revoked?

Q6: Why is it important in a good-list revocation scheme to keep hashes of the valid certificates, rather than just their serial numbers?