COMP 4334 Principles and Practice of Internet Security
Assignment 2

Q1 Answering the following short questions.

(1) What are the two essential security services provided by the SSL record protocol? And what are the techniques used to achieve the security services, respectively? [**4 marks**]

(2) What is the main difference between SSH and SSL regarding mutual authentication? [**4 marks**]

(3) List two major purposes of the SSL Handshake protocol. [**4 marks**]

Q2 Suppose a user A wants to send messages to n recipients $B_1, B_2, \cdots, B_n$. Each of the recipients B_i wants to make sure that the message she receives is indeed from A. So they decided to use a MAC scheme to achieve message authentication.

(1) Suppose that A has shared a secret key k with **all** the recipients. For every message m that A wants to send, A also attaches a MAC $\tau = MAC(k, m)$ to that message. Briefly explain why this scheme cannot achieve message authentication. [**2 marks**]

(2) Suppose user A has a set of secret keys $S = \{k_1, \cdots, k_p\}$. Each recipient B_i has a **subset** $S_i \subset S$ of the secret keys. When A broadcasts a message m to the recipients, A will attach p MACs $\tau_1, \cdots, \tau_p$ to the message m, where $\tau_j = MAC(k_j, m),\ j = 1, \cdots, p$. *A recipient B_i will accept the message only when all the MACs corresponding to the keys in her own key set S_i pass verification.*

So what condition should the subsets $S_1, \cdots, S_n$ satisfy to achieve message authentication (we assume that the recipients do not collude)? Also explain your answer [**6 marks**]

(3) Suppose $n = 10$ and $p = 5$, that is, there are 10 recipients and A has 5 secret keys. What are the secret keys for each recipient $S_1, \cdots, S_{10} \subset \{k_1, \cdots, k_5\}$ that meet the condition in (2)? [**4 marks**]

Q3 Suppose Alice uses textbook RSA signature without hashing. The public key is $PK = (n, e)$ and the secret key is $SK = (n, d)$.

(1) Suppose Eve knows the public information. Can Eve construct a pair of message and signature (i.e., (m, σ) to pass the verification? [**5 marks**]

(2) Now consider using a secure Hash function H to hash the message m before signing. Explain how adding the Hash operation could mitigate the problem in (1). [**5 marks**]

Q4 In public key distribution, a Certificate Authority (CA) will issue a certificate for each user. Explain how digital signature is used in this process and what functionality is achieved by digital signature. [**5 marks**]

Q5 The following mutual authentication and key exchange protocol uses public-key encryption to authenticate users and share a session key. Assuming that A and B reliably know each other's public key.
Notations: PU is public key; PR is private key; $E()$ is a public key encryption scheme; ID is identity; N_1 and N_2 are nonces.

- Step 1. $A \rightarrow B$: $E(PU_b, [N_1||ID_A])$. // note: $A \rightarrow B$ means A sends B a message
- Step 2. $B \rightarrow A$: $E(PU_a, [N_1||N_2])$.
- Step 3. $A \rightarrow B$: $E(PU_b, N_2)$.
- Step 4. $A \rightarrow B$: $E(PU_b, E(PR_a, K_s))$.

Questions:

(1) Explain how A can authenticate B. [**3 marks**]

(2) Explain how B can authenticate A. [**3 marks**]

(3) Explain the purposes of the two encryption operations in Step 4. [**5 marks**]