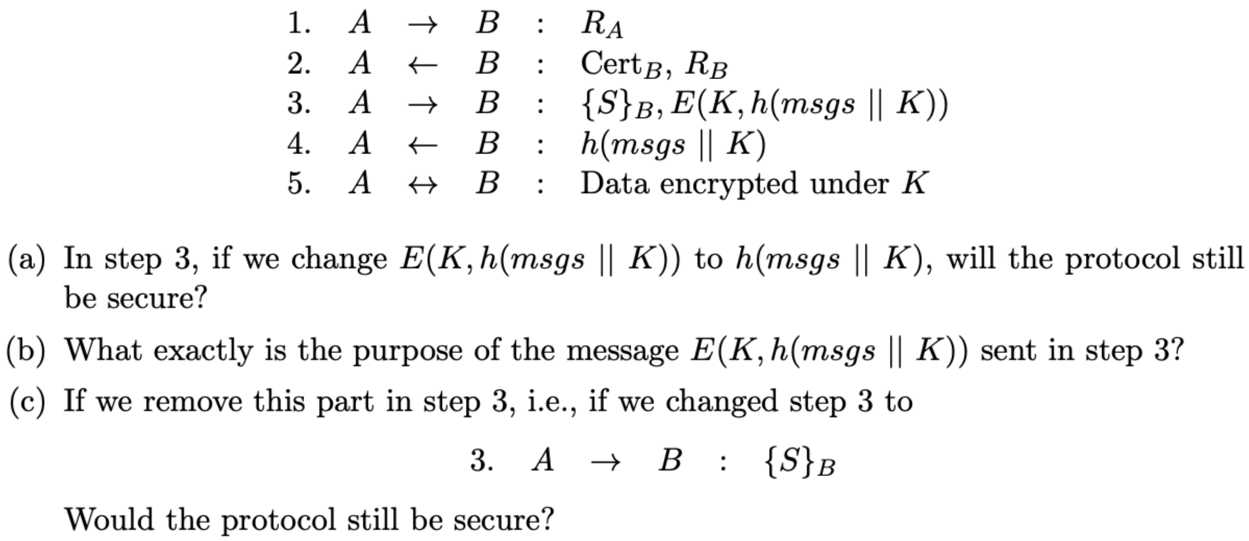
Network Security Technology

Tutorial 7, Week 7 (April 13) Due Date: April 20

薛春宇 518021910698

1. SSL (50 points)

Consider the SSL protocol shown below (with $K = h(S, R_A, R_B)$):



$$\begin{array}{lllll} 1. & A & \rightarrow & B & : & R_A \\ 2. & A & \leftarrow & B & : & \text{Cert}_B,\ R_B \\ 3. & A & \rightarrow & B & : & \{S\}_B, E(K, h(msgs \mid\mid K)) \\ 4. & A & \leftarrow & B & : & h(msgs \mid\mid K) \\ 5. & A & \leftrightarrow & B & : & \text{Data encrypted under } K \end{array}$$

(a) In step 3, if we change $E(K, h(msgs \mid\mid K))$ to $h(msgs \mid\mid K)$, will the protocol still be secure?

(b) What exactly is the purpose of the message $E(K, h(msgs \mid\mid K))$ sent in step 3?

(c) If we remove this part in step 3, i.e., if we changed step 3 to

$$3. \quad A \quad \rightarrow \quad B \quad : \quad \{S\}_B$$

Would the protocol still be secure?

Answer：

- (a) 协议还将安全。原因是只有 *B* 可以对 $\{S\}_B$ 进行解码，并生成正确的 $h(msgs \mid\mid K)$，因此 *Alice* 仍能够对 *Bob* 进行认证
- (b) 在步骤 *3* 中发送的 $E(K,\ h(msgs \mid\mid K))$ 可以使**拒绝服务攻击 (*DoS, Denial-of-Service*)** 更加困难。 如果删除该加密步骤，攻击者只需**在步骤 *3* 中向 *Bob* 发送一个随机数，然后放弃该连接，迫使 *Bob* 保持打开状态直到超时，这会浪费 *Bob* 一侧的资源**。 如果攻击者从不同来源重复多次，直至达到限制，*Bob* 将停止接受新的连接，*DoS* 攻击成功。
- (c) 协议还将安全。原因只有 *B* 可以对 $\{S\}_B$ 进行解码，但会对 *DoS* 攻击更加脆弱。

2 IKE (50 points)

In IKE Phase 1 digital-signature-based aggressive mode (see below), $proof_A$ and $proof_B$ are signed by Alice and Bob, respectively. However, in IKE Phase 1 public-key-encryption-based aggressive mode, $proof_A$ and $proof_B$ are neither signed nor encrypted. Explain why they can still securely perform the authentication.

Answer：

- 原因是，在基于公钥加密的主模式中，我们对 R_A 和 R_B 分别使用 *Bob* 和 *Alice* 的公钥进行了加密，只有使用对应的私钥才能解出 R_A 和 R_B，因此攻击者无法得知。而要想生成 *proof*，就必须要知道 *SKEYID*，进而必须要知道 R_A 和 R_B，因此该协议是安全的。