Homework 5

Pan Yisheng
515021910384

April 13, 2018

Problem 1. Key Exchange Consider the following protocol, where E is a symmetric key encryption scheme, and K is computed as $K = g^{ab}$.

$$A \to B : "I'm\ Alice", g^a$$
$$A \leftarrow B : "Bob", g^b, E_K([g^a, g^b]_{Bob})$$
$$A \to B : "Alice", E_K([g^a, g^b]_{Alice})$$

a) What is the long-term secret of this scheme?

b) Does the protocol support forward secrecy?

Solution Part a): The long-term secret of this scheme is the private key of A and B.

b): It depends on the security of symmetric key encryption scheme. Since attacker can gain the private key of A and B, he can gain two couples of plaintext and ciphertext: $E_K([g^a, g^b]_{Bob})$,$[g^a, g^b]_{Bob}$;$E_K([g^a, g^b]_{Alice})$,$[g^a, g^b]_{Alice}$. If the symmetric key encryption scheme is attacked with two couples of plaintext and ciphertext, it does't support forward secrecy. The prococol's problem is that it use session key instead of public key encryption to encrypt.

Problem 2. Authentication Consider the following protocol, where E is a symmetric key encryption scheme and K is a long-term symmetric key shared between A and B.

$$A \to B : "Alice", R_1$$
$$A \leftarrow B : R_2, E_K(R_1)$$
$$A \to B : E_K(R_2)$$

a) Does the scheme support session key establishment? If not, modify the protocol so that it does.

b) Does your protocol proposed in (a) support Perfect Forward Secrecy? If not, modify it so it supports PFS without adding any new encryption, digital signature or additional message flows.

Solution a): No,it doesn't. The modified protocol is

$$A \rightarrow B : \text{"}Alice\text{"}, R_1$$
$$A \leftarrow B : R_2, E_K(R_1, K_S)$$
$$A \rightarrow B : E_K(R_2)$$

b): No,it doesn't support PFS

$$A \rightarrow B : \text{"}Alice\text{"}, R_1$$
$$A \leftarrow B : R_2, E_K(R_1, g^b \ mod \ p)$$
$$A \rightarrow B : E_K(R_2, g^a \ mod \ p)$$