ELE2742 / ENG1467 - PUC-Rio, 2019.1

Lecture 3: Key Exchange Protocol

DATE

Lecturer: Yi-Fan Tseng *Scribe: Yi-Fan Tseng*

1 The Key Distribution Problem

Image that we are living in a city with high crime rate. Anything will be stolen if they are not properly secured. For example, packages will be opened by couriers if they are not locked. One day, Alice wants to send to Bob a valuable watch as a gift. To prevent the watch from being stolen, she

1. first puts the watch in a box;
2. then locks the box;
3. finally sends the box to Bob.

After receiving the locked box from Alice, however, Bob needs the key to Alice's lock to open the box. The problem is how Alice to give the key to Bob.

Solution 1. A straightforward solution is that, Alice meets Bob at some time and give the key directly to Bob. Nevertheless, it would be meaningless to send the locked box if Alice is able to meet Bob.

Solution 2. Another method is that Alice sends the key to Bob. In order to prevent the key from being stolen, Alice needs to find another box and then lock the key in this box with another lock. However, it would be meaningless since Bob is still unable to open the new box due to the lack of the key to the new box.

It is the *key distribution problem* in classical cryptography. In a war, when a commander wants to send a message to another commander, the message should be encrypted to prevent it from being eavesdropped. However, how to share the key for encrypting the message. How to securely deliver the key hence becomes an important issue in communication.

In 1976, Diffie and Hellman [1] in their pioneering paper proposed a new idea to solve the key distribution problem. Consider the aforementioned scenario. Alice performs the same as we just mentioned. After receiving the locked box, Bob performs as follows.

1. Bob locks the box with his own lock.

2. Bob then sends the "doubly locked" box back to Alice.

After Alice receives the box, she unlocks her lock, and sends the box to Bob again. Note that, now the box is locked with only Bob's lock, and thus Bob is able to obtain the gift by unlocking the box with his own key.

The operation of locking a box can be viewed as a function in mathematics. To choose a lock can be analogue to choose a function. Therefore, the aforementioned scenario can be rewritten as follows. Alice and Bob choose their own functions F_A and F_B with restrictions that

1. given $F_A(x)$ or $F_B(x)$, it is hard to find x (a lock should be hard to open without the corresponding key);
2. $F_B^{-1}(F_A^{-1}(F_B(F_A(x)))) = x$, which is equivalent to $F_B(F_A(x)) = F_A(F_B(x))$.

The solution proposed by Diffie and Hellman is the famous *Diffie-Hellman Key Exchange Protocol*.

2 Diffie-Hellman Key Exchange Protocol

2.1 Deffie-Hellman Key Exchange Protocol

The Diffie-Hellman key exchange (DHKE) protocol is performed as follows.

Alice and Bob first setup the system parameter together.

1. Choose a large prime p such that $p-1$ has a prime factor q.
2. Let $\mathbb{G}$ is a subgroup of $\mathbb{Z}_p^*$. Find the generator g of $\mathbb{G}$. Such $\mathbb{G}$ exists since $|\mathbb{Z}_p^*| = p-1$ and $q|p-1$.

After deciding the system parameter $(\mathbb{G}, g, p)$, Alice and Bob choose their own secret x_A and x_B from $\mathbb{Z}_q^*$, and compute $y_A = g^{x_A} \mod p$ and $y_B = g^{x_B} \mod p$. Next, Alice sends y_A to Bob, and Bob sends y_B to Alice. Finally, Alice computes $k_A = y_B^{x_A} \mod p$ and Bob computes $k_B = y_A^{x_B} \mod p$.

Alice		Bob
$x_A \xleftarrow{\$} \mathbb{Z}_q^*$		$x_B \xleftarrow{\$} \mathbb{Z}_q^*$
$y_A = g^{x_A} \mod p$	$\xleftarrow{y_A}$	$y_B = g^{x_B} \mod p$
	$\xrightarrow[y_B]{}$	
$k_A = y_B^{x_A} \mod p$		$k_B = y_A^{x_B} \mod p$

Correctness.

$k_A = y_B^{x_A} \pmod p = (g^{x_B})^{x_A} \pmod p = g^{x_A x_B} \pmod p = (g^{x_A})^{x_B} \pmod p = y_A^{x_B} \pmod p = k_B$

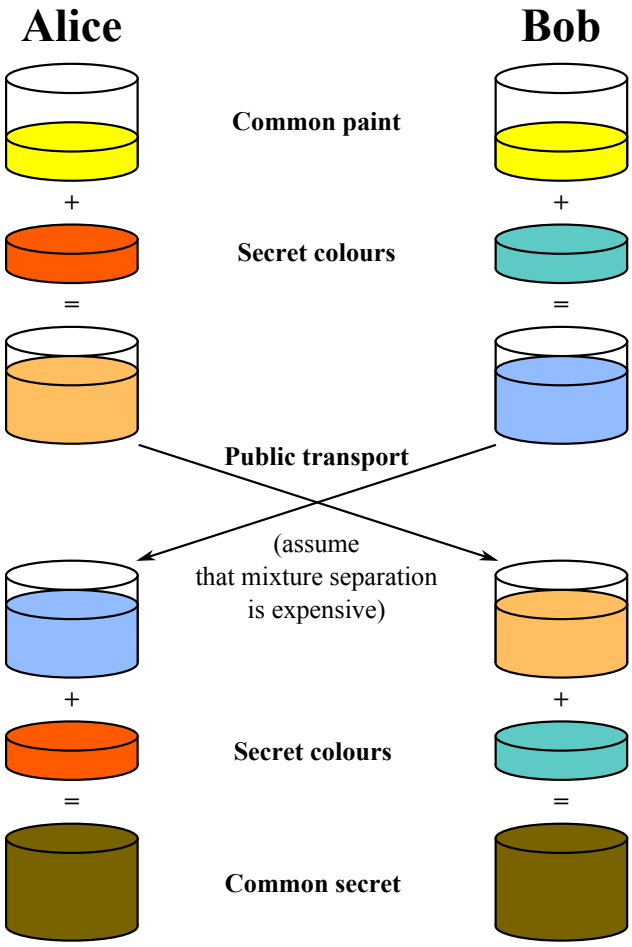

Figure 1: Diffie-Hellman Key Exchange Protocol (Wiki)

Fig 1 shows an illustration for Diffie-Hellman key exchange protocol.

2.2 Security Analysis

We then give the security analysis for the DHKE protocol. Assume that there is an attacker Eve who eavesdrops the communications and wants to establish the shared key k_A (or k_B). From eavesdropping the communication, Eve can obtain y_A and y_B. Note that Eve needs x_A (resp. x_B) to recover k_A (resp. k_B). However, it is hard to recover x_A given g, y_A, p, since it is equivalent to solve the discrete log problem. The case of recovering x_B is similar. Besides, with only y_A and y_B, Eve can only compute $y_A * y_B = g^{x_A+x_B}$ or $y_A/y_B = g^{x_A-x_B}$.

2.3 Vulnerability

Though the DHKE protocol allows two parties to construct a shared key via a public channel, it is vulnerable to the *man-in-the-middle* attacks (MITM). Intuitively speaking, MITM is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. In the scenario shown above, Eve may choose her (y_E, x_E), and act as a man in the middle to perform the DHKE protocol to Alice and Bob separately. Thus Alice would think that she is communicating to Bob, and Bob would think that he is communicating to Alice, but they are actually communicating with Eve. Finally, Eve is able to establish shared keys with both Alice and Bob. Therefore, Eve can obtain the massage transmitted between Alice and Bob. To solve the problem, we can adopt the following solutions.

- Authentication
- Time Stamp
- Certificate

3 One Round, 3-Party Key Exchange Protocol

In 2004, Joux [2] proposed a key exchange protocol allowing three parties to agree on a shared key in one round. It can be regarded as an extension of the DHKE protocol using pairings.

Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a bilinear map, where $\mathbb{G}, \mathbb{G}_T$ are multiplicative groups of prime order p, and g be a generator of $\mathbb{G}$. Figure 2 shows the details of Joux's scheme.

Correctness.

$$K_A = e(y_B, y_C)^{x_A} = e(g^{x_B}, g^{x_C})^{x_A} = e(g, g)^{x_A x_B x_C}$$
$$K_B = e(y_A, y_C)^{x_B} = e(g^{x_A}, g^{x_C})^{x_B} = e(g, g)^{x_A x_B x_C}$$
$$K_C = e(y_A, y_B)^{x_C} = e(g^{x_A}, g^{x_B})^{x_C} = e(g, g)^{x_A x_B x_C}$$

The security analysis is similar to the DHKE protocol.

References

[1] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theor.*, 22(6):644–654, Sept. 2006.

[2] A. Joux. A one round protocol for tripartite Diffie–Hellman. *Journal of Cryptology*, 17(4):263–276, Sep 2004.

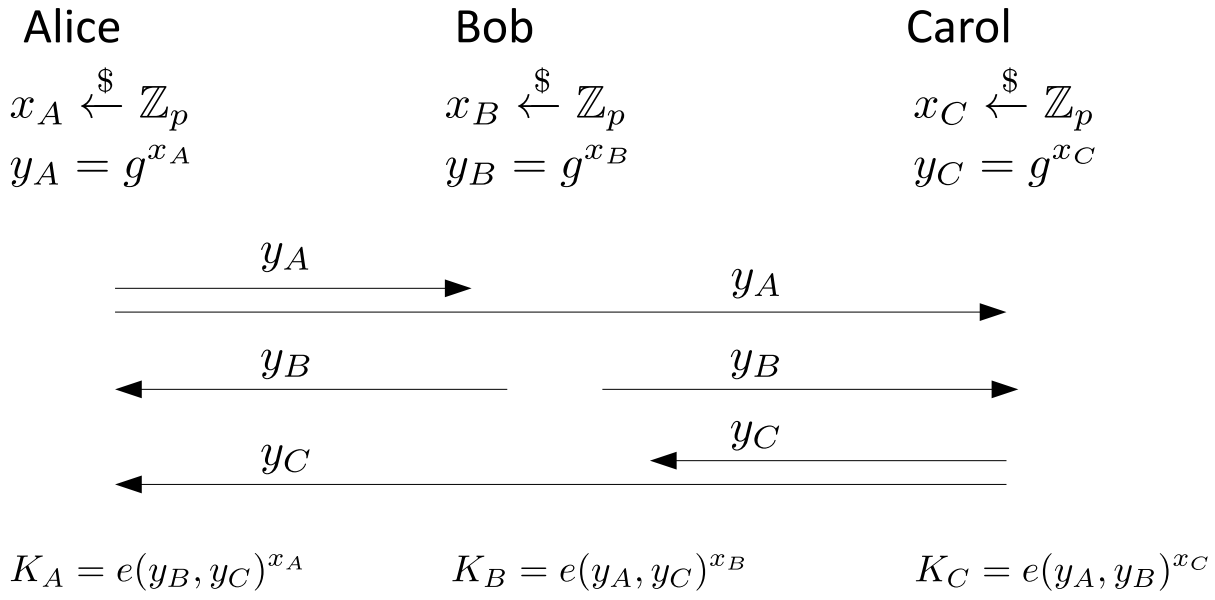

Figure 2: Joux's Key Exchange Protocol