密钥交换与秘密共享

Diffie-Hellman密钥交换（重点）

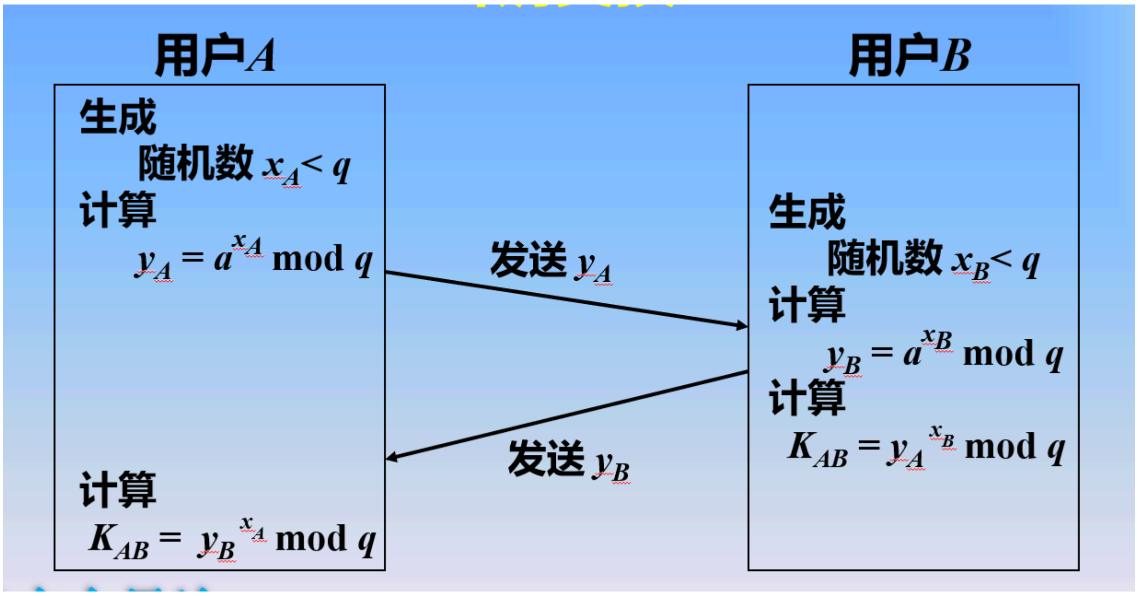
- 定义：一个密钥分发策略，用于生成临时会话密钥。
  - 不能用于交换任意消息
  - 只可以建立一个共同的会话密钥
  - 只有参与的双方才可以知道会话的密钥值
- 基于在有限域的模素数或多项式运算，运算简单
- 安全依赖于计算离散对数难题，破解困难
- 交换步骤：

- **所有用户都同意以下全局参数：**
  - **大素数或者多项式** q
  - a **是模**q**下的一个原始根**
- **每一个用户(例如** A**和**B**) 产生他们的密钥**
  - **选择一个私钥(数字)：** $x_A < q$ ， $x_B < q$
  - **计算公开密钥：** $y_A = a^{x_A} \bmod q$， $y_B = a^{x_B} \bmod q$
- **公开密钥(**y_A**和**y_B **)，保留私钥(**x_A**和**x_B **)**

- **用户**A**和**B **共享会话密钥** K_{AB}**:**

$$
\begin{aligned}
K_{AB} &= a^{x_A x_B} \bmod q \\
&= y_A^{x_B} \bmod q \quad (B \text{ 使用这个公式计算}) \\
&= y_B^{x_A} \bmod q \quad (A \text{ 使用这个公式计算})
\end{aligned}
$$

- K_{AB} **作为会话密钥，可以在A 和 B之间采用私钥加密方案中使用。**
- **如果 A 和 B 接着通信, 他们将会采用同样的密钥，除非他们选择新的公钥。**



- 例子

假设用户 A 和 B 想要交换会话密钥，并同意素数 q=353 和 a=3，之后A和B分别选择随机私钥:

$$A \text{ 选择 } x_A=97,\ B \text{ 选择 } x_B=233$$

并计算各自的公钥发送给对方

A 计算 $y_A=3^{97} \bmod 353 = 40$　B计算 $y_B=3^{233} \bmod 353 = 248$

收到公钥后，A和B分别计算会话密钥:

A 计算 $K_{AB}=y_B^{x_A} \bmod 353 = 248^{97} = 160$

B 计算 $K_{AB}=y_A^{x_B} \bmod 353 = 40^{233} = 160$

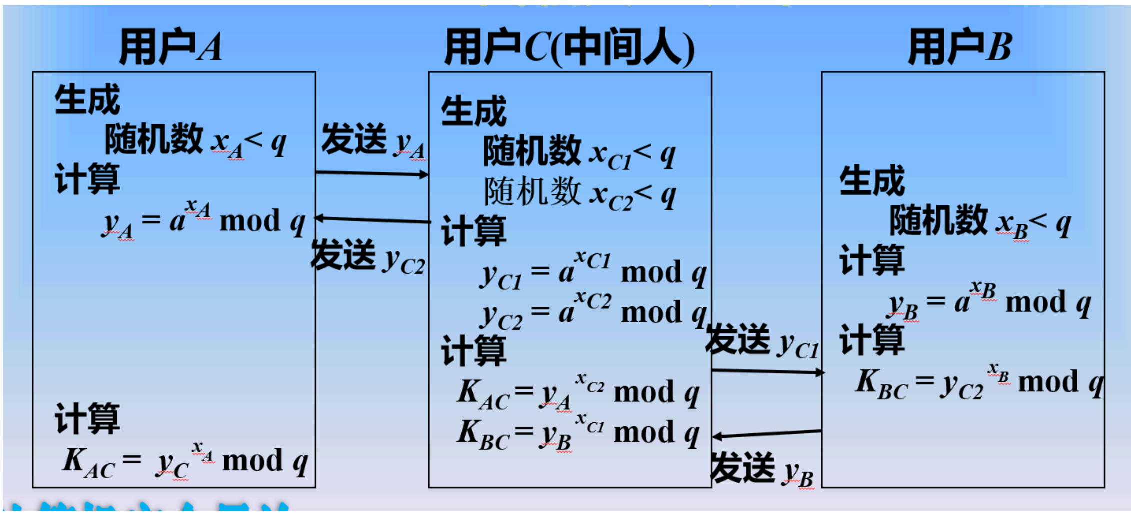
- 安全分析

由于x_A，x_B为私有，攻击者只能利用公开密钥和参数进行攻击，如a, q, y_A和y_B。为此攻击者必须求离散对数才能确定密钥:

$$x_B = d\log_{a,q}(y_B)$$

Diffie-Hellman的安全性在于，虽然计算模幂运算相对容易，但计算离散对数却非常困难。对于大素数，计算离散对数被认为是不可行的。

- 但是Diffie-Hellman容易受到“中间人攻击”。“中间人攻击”可以窃听信息，也可以修改信息，需要添加认证功能才可以防止攻击。



- 一种简单的解决思路：将用户的公/私密钥存在一个目录里并公布，用户可以查询和请求实现安全通信。任何时候用户*B*都可以访问*A*的公开密钥，从而计算会话密钥，再使用它给*A*发送加密信息。这种通信方式不仅可以提供保密性，还能提供一定程度的认证，但仍不能防止重放攻击。

Shamiar密钥共享（了解）

- 定义：将秘密*K*分发给*n*个人，当中的任意*t*个人聚集在一起可以恢复出密钥*K*，并用于加/解密信息，而任意*t*-1个人则无法恢复密钥*K*。
- 共享步骤

假设有秘密K，任取随机数$a_1, a_2, \dots, a_{t-1}$，通过构造如下多项式：

$$f(x) = K + a_1 x + \dots + a_{t-1} x^{t-1}$$

其中所有的运算都在有限域F中进行，任取n个数$x_1, x_2, \dots, x_n$分别带入多项式得到$f(x_1), f(x_2), \dots, f(x_n)$，并将$(x_1, f(x_1)), (x_2, f(x_2)), \dots, (x_n, f(x_n))$分发给$n$个用户。

$$\begin{bmatrix} 1 & x_1 & \dots & x_1^{t-1} \\ 1 & x_2 & \dots & x_2^{t-1} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 1 & x_t & \dots & x_t^{t-1} \end{bmatrix} \begin{bmatrix} K \\ a_1 \\ a_2 \\ \dots \\ a_{t-1} \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \dots \\ \dots \\ y_{t-1} \end{bmatrix} \Rightarrow \begin{bmatrix} K \\ a_1 \\ a_2 \\ \dots \\ a_{t-1} \end{bmatrix} = \begin{bmatrix} 1 & x_1 & \dots & x_1^{t-1} \\ 1 & x_2 & \dots & x_2^{t-1} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 1 & x_t & \dots & x_t^{t-1} \end{bmatrix}^{-1} \begin{bmatrix} y_1 \\ y_2 \\ \dots \\ \dots \\ y_{t-1} \end{bmatrix}$$