现代密码学

第五十讲 Diffie-Hellman 密钥交换

信息与软件工程学院

第五十讲 Diffie-Hellman 密钥交换

- Diffie-Hellman密钥交换协议
- Diffie-Hellman密钥交换中的安全问题

Diffie-Hellman密钥交换协议

密钥交换是实现安全通信的基础

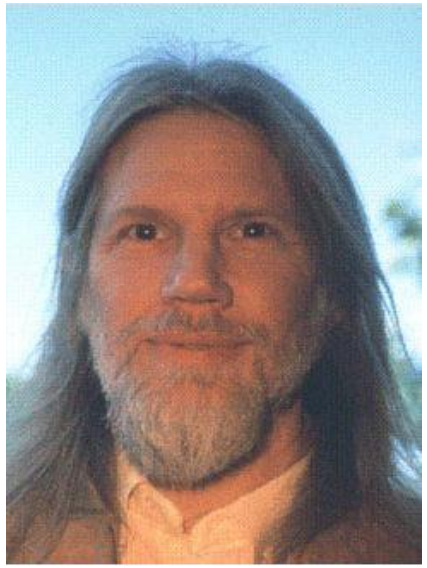
- ✓ 商用加密算法AES和DES需要在安全通信之前，实现通信双方的密钥共享。

密钥交换的方法：

- ✓ 基于**RSA**的密钥交换；
- ✓ 基于**KDC**技术 **(Key Distributed Center，** 密钥分发中心**)**；
- ✓ **Diffie-Hellman**密钥交换（简称：**DH**算法）；
- ✓ 基于物理层的密钥交换。

Diffie-Hellman密钥交换协议

- **DH算法**是不安全信道下实现安全密钥共享的一种方法，由 W. Diffie 和 M. Hellman 在1976年提出的第一个公开的公钥密码算法。

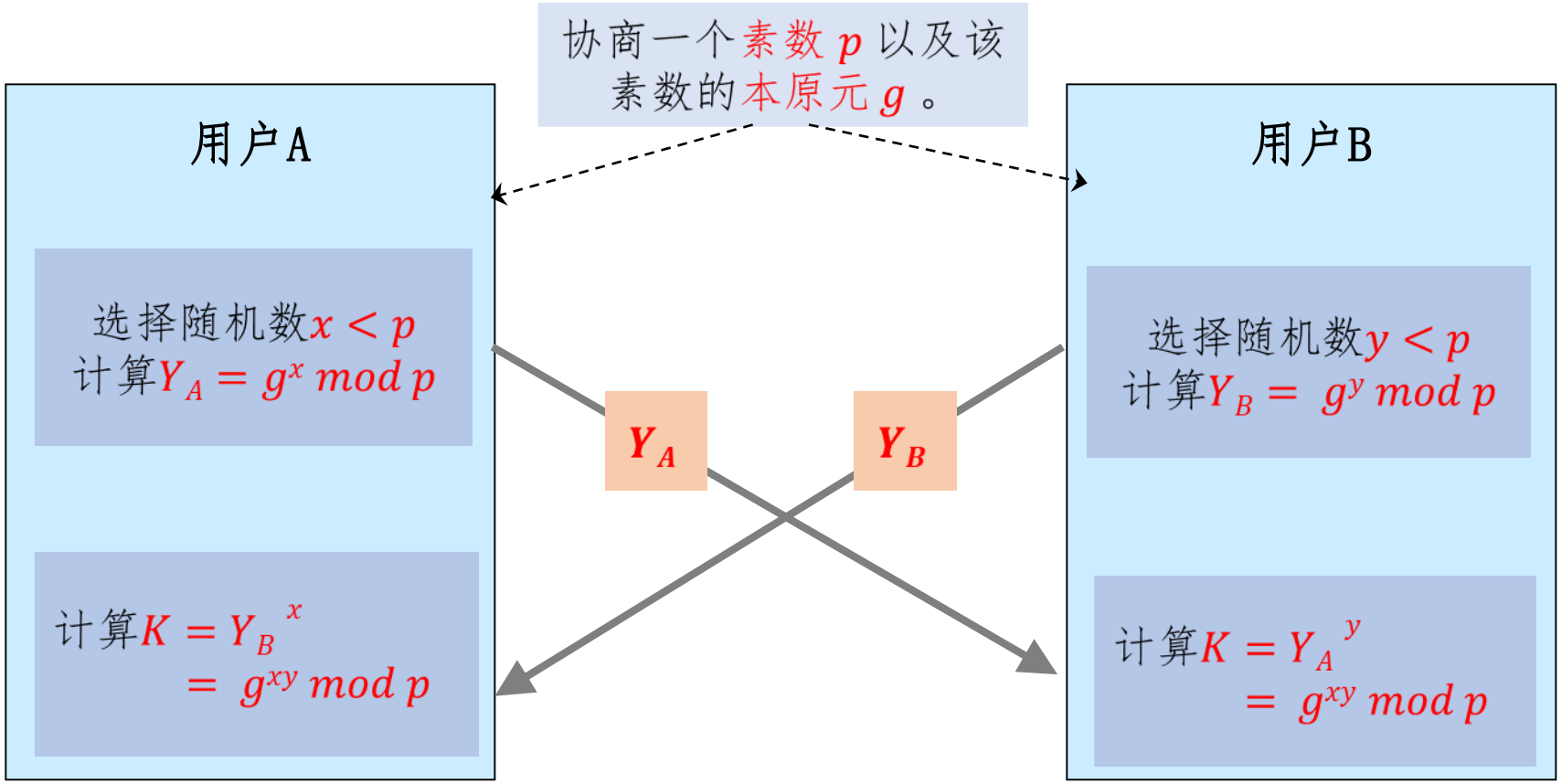


Whitfield Diffie

Martin Hellman

Diffie-Hellman密钥交换协议

DH算法



Diffie-Hellman密钥交换协议

DH协议的例子：

- ✓ 假设素数 $p = 97$，其本原元 $g = 5$
- ✓ 若用户A和B的选取的随机数分别为：$x = 36$；$y = 58$
- ✓ 用户A计算：$Y_A = 5^{36} \bmod 97 = 50 \bmod 97$
- ✓ 用户B计算：$Y_B = 5^{58} \bmod 97 = 44 \bmod 97$
- ✓ 用户A计算密钥：$K = 44^{36} \bmod 97 = 75 \bmod 97$
- ✓ 用户B计算密钥：$K = 50^{58} \bmod 97 = 75 \bmod 97$

第五十讲 Diffie-Hellman 密钥交换

- Diffie-Hellman密钥交换协议
- Diffie-Hellman密钥交换中的安全问题

Diffie-Hellman密钥交换中的安全问题

◘安全性分析

- ✓ 攻击者可利用的信息包括素数 p 、本原元 g、中间值Y_A和Y_B.
- ✓ 若攻击者想要获取密钥K，必须通过

$$Y_A = g^x \bmod p \quad 和 \quad Y_B = g^y \bmod p$$

计算x和y，这是一个离散对数求解问题。

- ✓ 因此，算法的安全性基于求离散对数的困难性。

除了破获密钥，攻击者还有其他的攻击方式吗？

Diffie-Hellman密钥交换中的安全问题

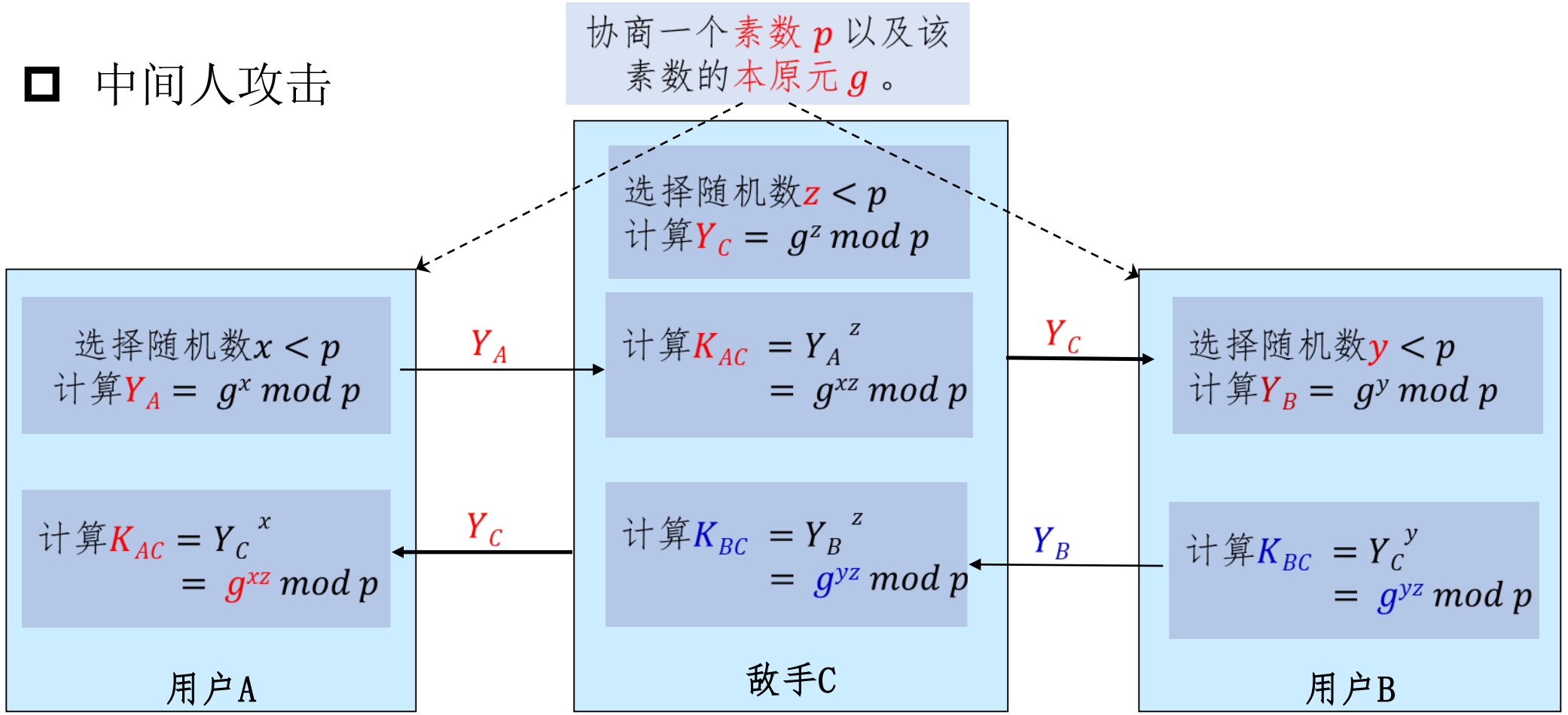
- DH算法存在的安全问题：

  ✓容易遭受阻塞攻击：因为幂运算是计算密集性的，当敌手发起大量的密钥请求，受攻击者将花费较大计算资源来做幂运算；

  ✓容易遭受中间人攻击：敌手可分别冒充用户A和B中的一方，与另一方交换密钥（敌手就可以监听和传递A和B的秘密信息而不被发现）。

Diffie-Hellman密钥交换中的安全问题

- 中间人攻击



Diffie-Hellman密钥交换中的安全问题

- 课后调研：
  - ✓ 了解一下奥克利（**Oakley**）协议是什么？
  - ✓ **Oakley**协议是如何解决**DH**协议所面临的几个安全问题的？

感 谢 聆 听!

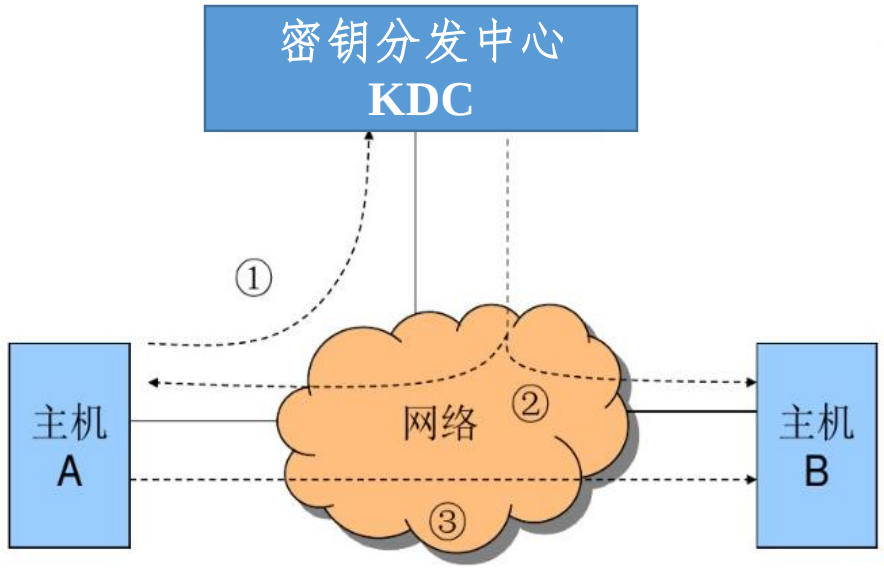
djchen@uestc.edu.cn

端到端密钥交换

- 密钥交换是实现安全通信的基础

✓ 基于**RSA**：证书颁发机构 **CA (Certificate Authority)**；

✓ 基于**DES/AES**：密钥分发中心 **KDC (Key Distributed Center)**。



端到端密钥交换

- 端到端密钥交换

  随着物联网的兴起，端到端的安全通信成为必然需求。

- Diffie-Hellman (DH)密钥交换协议

一种端到端的密钥交换协议，它允许两个终端生成相同的共享密，而不需要第三方协助。

- 通常用于密钥的交换，常用到 DH 的情况个示例：
  - 使用 IPsec VPN 交换数据
  - 使用 SSL 或 TLS 在互联网中加密数据
  - 交换 SSH 数据

端到端协议

- 1992年，Diffie、Oorschot和Wiener提出了一个端到端协议（station-to-station protocol）