PART 8

其他公钥密码体制

8.1 Diffie-Hellman密钥交换

8.1 Diffie-Hellman密钥交换

- 第一个公钥算法
- 1976由Diffie 和 Hellman 提出
- DH算法是一个实用的密钥公开交换算法
- 算法本身只限于进行密钥交换
- 已应用在许多商业产品中

8.1 Diffie-Hellman密钥交换

- 是一个公钥分配方案
  - 不能用于交换任意的消息
  - 只限于进行公共密钥的建立
  - 只对通信的双方已知
- 密钥的值依赖于通信的参与者 (以及他们的私钥和公钥信息)
- 有限域中的指数运算（模一个素数）是相对容易的，而离散对数的计算是相对困难的。

8.1 Diffie-Hellman密钥交换

Diffie-Hellman的建立

- 所有用户均已知全局参数:
  - 一个大素整数(或多项式)：q
  - 一个模 q 的本原根：α
- 每个用户 (如 A) 产生自己的密钥
  - 选择一个保密的随机数: $x_A < q$
  - 计算其公钥: $y_A = \alpha^{x_A} \bmod q$
- 每个用户公开其公钥 y_A

8.1 Diffie-Hellman密钥交换

- 用户A 和 B共享的会话密钥是 K_{AB}:

$$K_{AB} = \alpha^{x_A.x_B} \bmod q$$

$$= y_A^{x_B} \bmod q \quad \text{(which B can compute)}$$

$$= y_B^{x_A} \bmod q \quad \text{(which A can compute)}$$

- 会话密钥K_{AB} 作为A和B两个用户在传统密码体制中的**共享密钥**来使用的
- 可以一直使用前面产生的会话密钥，直到想重新选择新的会话密钥为止。
- **攻击者需要解出x, 必须求解离散对数**。

Alice

Bob

Alice		Bob
Alice和Bob共享一个素数q以及整数α（$\alpha<q$）且α是q的本原根		Alice和Bob共享一个素数q以及整数α（$\alpha<q$）且α是q的本原根
Alice产生一个私钥X_A使得$X_A<q$		Bob产生一个私钥X_B使得$X_B<q$
Alice计算公钥$Y_A=\alpha^{X_A} \bmod q$	Y_A	Bob计算公钥$Y_B=\alpha^{X_B} \bmod q$
Alice收到Bob的公钥Y_B	Y_B	Bob收到Alice的公钥Y_A
Alice计算共享密钥$K=(Y_B)^{X_A} \bmod q$		Bob计算共享密钥$K=(Y_A)^{X_B} \bmod q$

8.1 Diffie-Hellman密钥交换

Diffie-Hellman 举例

- 用户 Alice 和 Bob 想交换密钥:
- 双方同意使用全局参数 $q = 353$ 和$\alpha=3$
- 随机选择一个保密的私钥:
  - A 选择 $x_A = 97$, B 选择 $x_B = 233$
- 分别计算各自的公钥:
  - $y_A=3^{97} \bmod 353 = 40$ (Alice)
  - $y_B=3^{233} \bmod 353 = 248$ (Bob)
- 计算共享的会话密钥:
  - $K_{AB}= y_B^{x_A} \bmod 353 = 248^{97} = 160$ (Alice)
  - $K_{AB}= y_A^{x_B} \bmod 353 = 40^{233} = 160$ (Bob)

8.1 Diffie-Hellman密钥交换

海南大学 Hainan university

密钥交换协议

- 用户在每一次通信时都产生随机的公开的和保密的DH密钥对
- 用户产生D-H密钥对，并公开其公钥在一个目录中，需要与其进行保密通信时，查询并使用这个目录。
- 上述两种情况都存在中间人攻击
- 认证是需要的

8.1 Diffie-Hellman密钥交换

DH交换的中间人攻击

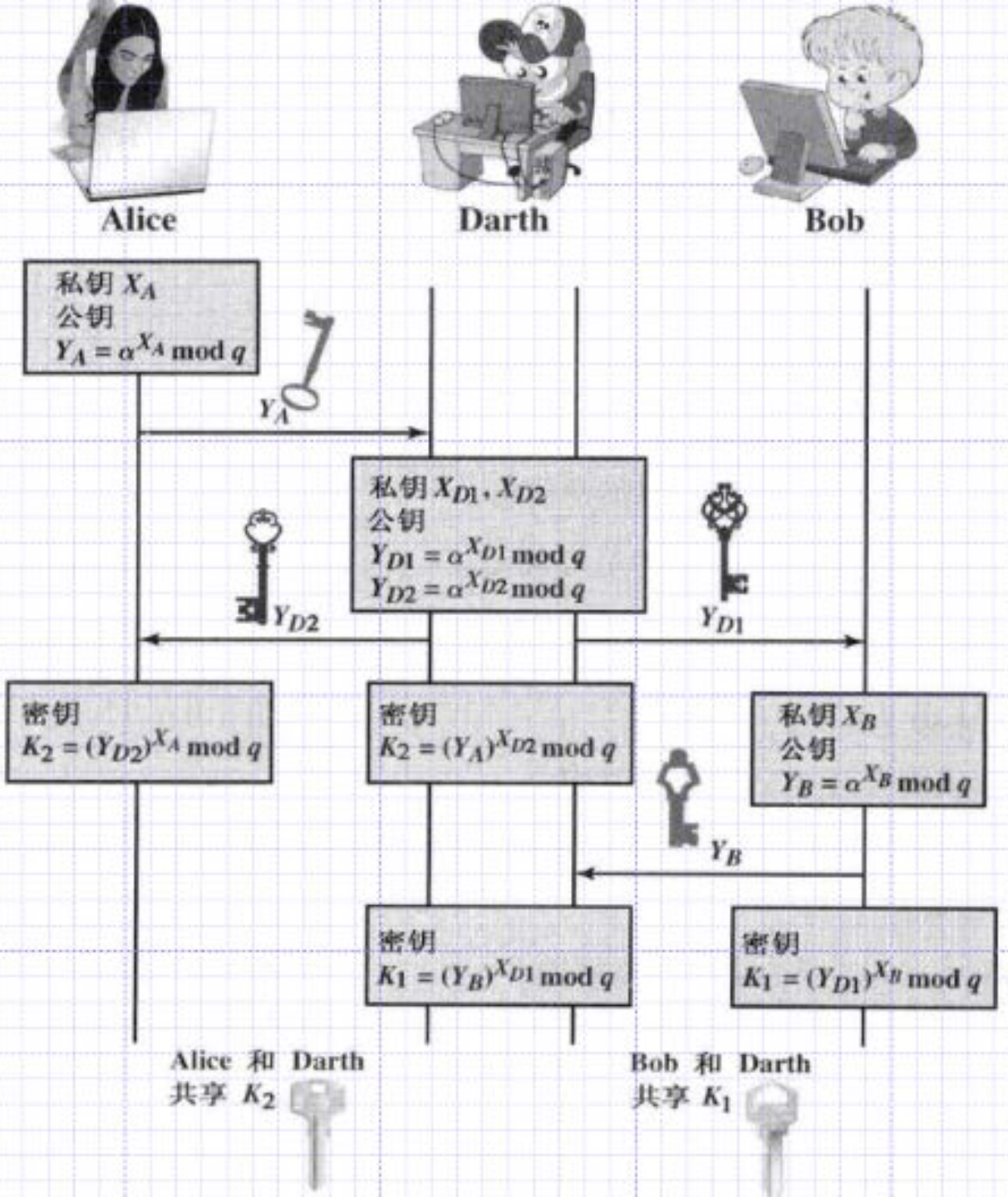
- (1) Darth生成两个随机数X_{D1}和X_{D2}，随后计算相应的公钥Y_{D1}和Y_{D2}；
- (2) Alice将Y_A传递给Bob；
- (3) Darth截获了Y_A，将Y_{D1}传给Bob，同时计算

$$K_2 = (Y_A)^{X_{D2}} \bmod q$$

- (4) Bob收到Y_{D1}，计算 $K_1 = (Y_{D1})^{X_B} \bmod q$
- (5) Bob将Y_B传给Alice；
- (6) Darth截获了Y_B，将Y_{D2}传给Alice，Darth计算

$$K_1 = (Y_B)^{X_{D1}} \bmod q$$

- (7) Alice收到Y_{D2}，计算 $K_2 = (Y_{D2})^{X_A} \bmod q$



8.1 Diffie-Hellman密钥交换

海南大学 Hainan university

DH交换的中间人攻击

- (1) Alice 发送机密消息 M： $E(K_2, M)$；
- (2) Darth 截获了该消息，解密，恢复出M；
- (3) Darth 将$E(K_1, M)$或 $E(K_1, M')$发送给Bob。

增强安全性：增加A与B的认证，用公钥证书或者共享密钥

8.2 ElGamal密码

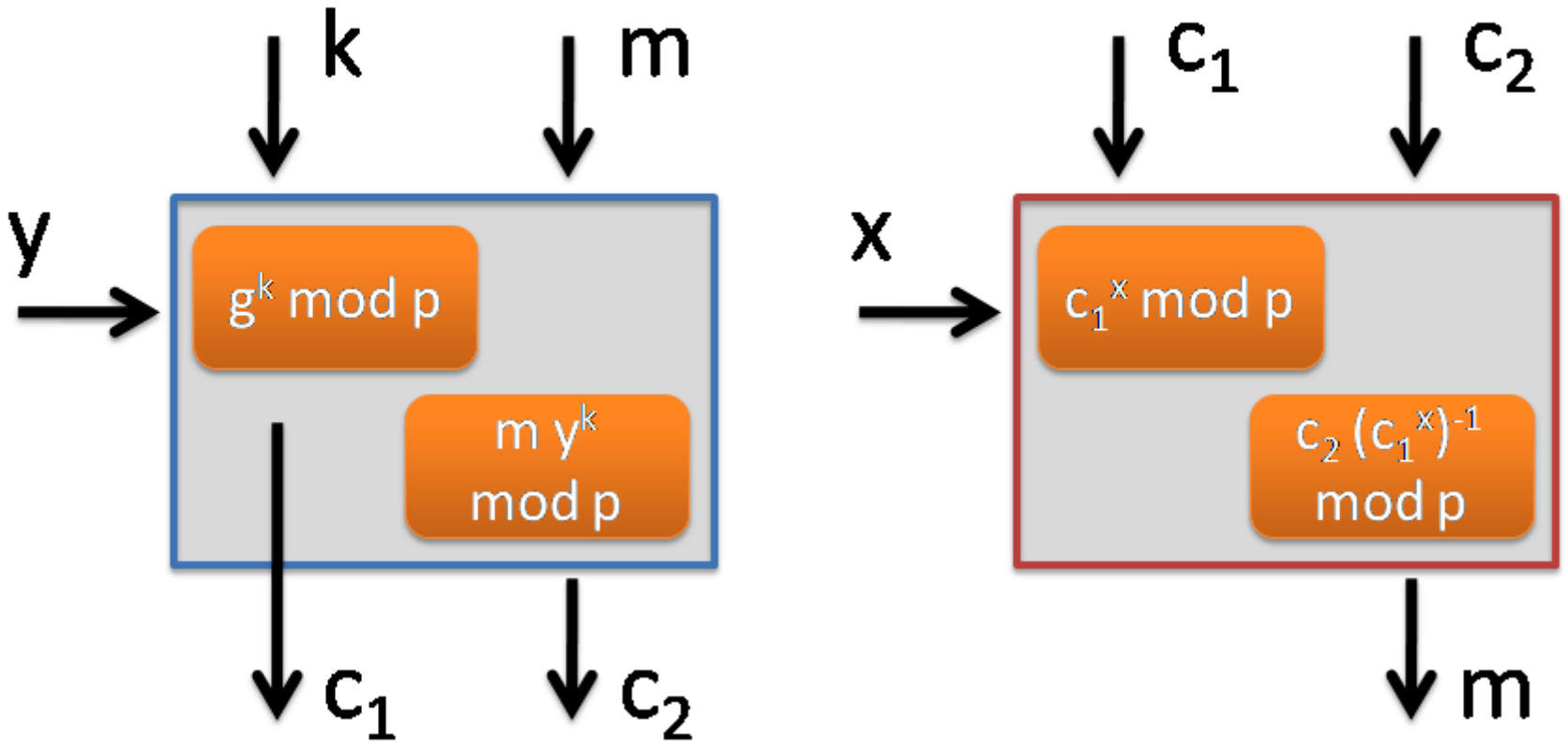
8.2 ElGamal密码

- Taher Elgamal在1984和1985年间提出了一种基于离散对数问题的公钥密码体系，其类似于Diffie-Hellman的密钥协商协议。

8.2 ElGamal密码

ElGamal算法

- p:prime, g:<g>=Z_p^*, pk=y=g^x, sk=x



8.2 ElGamal密码

ElGamal举例-加密

- Alice选择X_A=5，α = 10；
- 计算$Y_A = \alpha^{X_A} \bmod q = \alpha^5 \bmod 19 = 3$
- Alice的私钥为5；公钥为 $\{q, \alpha, Y_A\} = \{19, 10, 3\}$
- 假如Bob想将值M=17发送，则作如下计算：
  - (1) Bob选择 $k = 6$
  - (2) 计算 $K = (Y_A)^k \bmod q = 3^6 \bmod 19 = 729 \bmod 19 = 7$
  - (3) 计算 $C_1 = \alpha^k \bmod q = 10^6 \bmod 19 = 11$

    $C_2 = KM \bmod q = 7 \times 17 \bmod 19 = 119 \bmod 19 = 5$
  - Bob发送密文（11, 5）

8.2 ElGamal密码

ElGamal举例-解密

- **Alice选择** $K = (C_1)^{X_A} \bmod q = 11^5 \bmod 19 = 7$
- **在GF(19) 中** $K^{-1} = 7^{-1} \bmod 19 = 11$
- **计算** $M = (C_2 K^{-1}) \bmod q = 5 \times 11 \bmod 19 = 17$

8.2 ElGamal密码

练习

试在 mod 17 （q=17）的情况下验证ElGamal加解密方案（明文，密钥 自行选择）。

（1）g_1=2

（2）g_2=3

8.2 ElGamal密码

练习

试在 mod 17 （q=17）的情况下验证ElGamal加解密方案（明文，密钥 自行选择）。

（1）g_1=2，取x=2，则y=2^2=4， 取k=4，则

C2=my^k=m 4^4= m mod17

（2）g_2=3 (3 是生成元，不存在上述问题)

8.2 ElGamal密码

安全性

- 破解ElGamal相当于解Diffie-Hellman问题。
- ElGamal的安全性依赖于Z_p^*上的离散对数问题;
- 在加密过程中，对不同的消息m都应选取不同的随机数k，否则，攻击者可以很容易攻击ElGamal公钥体系。

8.2 ElGamal密码

攻击举例-k

- 如果k用于多个分块，利用信息的分块m_1，攻击者计算

$$C_{1,1} = \alpha^k \bmod q; C_{2,1} = KM_1 \bmod q$$

$$C_{1,2} = \alpha^k \bmod q; C_{2,2} = KM_2 \bmod q$$

- 于是

$$\frac{C_{2,1}}{C_{2,2}} = \frac{KM_1 \bmod q}{KM_2 \bmod q} = \frac{M_1 \bmod q}{M_2 \bmod q}$$

- 若M_1已知，很容易计算M_2

$$M_2 = (C_{2,1})^{-1} C_{2,2} M_1 \bmod q$$

8.2 ElGamal密码

海南大学 Hainan university

ElGamal etc

- 缺点
  - 需要随机数
  - 密文长度加倍
- ElGamal可以迁移到ECDLP上
- ElGamal签名和DSS（数字签名标准）


海南大学
Hainan university