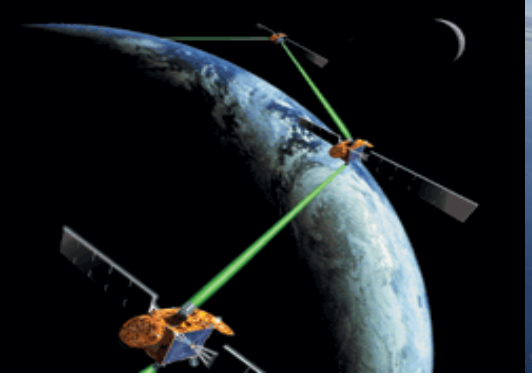
普通高等教育“十一五”国家级规划教材
教育部2011年精品教材

网络安全—技术与实践（第2版）

刘建伟 王育民 编著

清华大学出版社




课件制作人声明

- 本课件总共有17个文件，版权属于刘建伟所有，仅供选用此教材的教师和学生参考。
- 本课件严禁其他人员自行出版销售，或未经作者允许用作其他社会上的培训课程。
- 对于课件中出现的缺点和错误，欢迎读者提出宝贵意见，以便及时修订。

课件制作人：刘建伟

2016年10月11日

电子商务：如何确保账户信息安全？

amazon.com

天猫 TMALL.COM

PayPal

支付宝™

淘宝网
Taobao.com

JD.京东.COM

双钥密码体制（一）

一 公钥密码体制的基本概念

二 RSA公钥密码算法

三 ElGamal公钥签名算法

四 其它公钥密码

专题：双钥密码体制（一）

一 公钥密码体制的基本概念

二 RSA公钥密码算法

三 ElGamal公钥签名算法

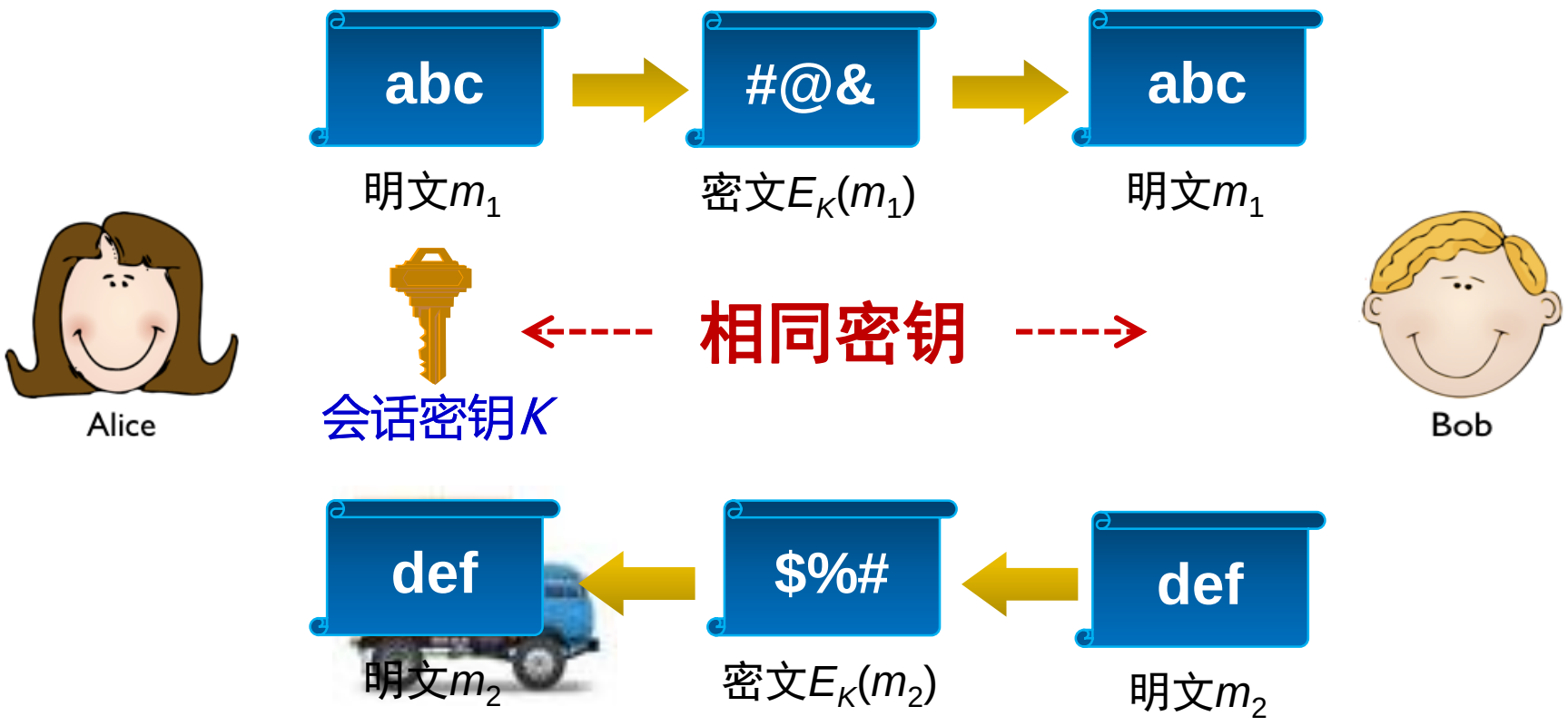
四 其它公钥密码

1.1 公钥密码的历史

- 1968年，ARPA启动“资源共享计算机网络”建设项目，建成了ARPANET，将4所大学的计算机联网。40年多来，随着因特网的迅猛发展，其商业应用得到普及，迫切需要解决保密通信问题。
- 1976年，美国斯坦福大学电气工程系的研究员Diffie和Hellman教授在奠基性论文 “密码学的新方向”中提出公开密钥密码体制的概念，旨在解决网络通信的两大安全问题：保密与认证。
- 公钥密码体制的基础，是计算复杂度理论。
  - ✓ 单向函数/单向陷门函数
  - ✓ 计算上困难问题/NP完全问题

为什么需要公钥密码——单钥体制的不足

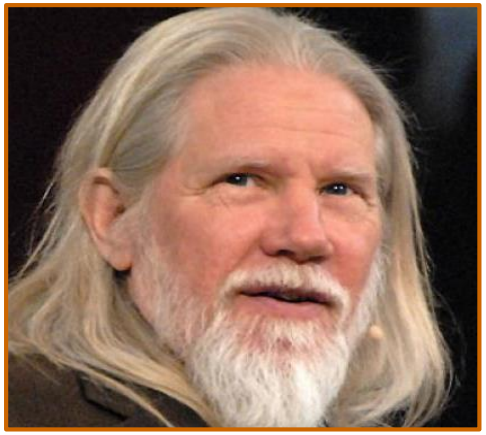
回顾：对称（单钥）密码体制



1.2 公钥密码学

D-H算法的设计者

1976年，美国的两位著名的密码学家W. Diffie和M. Hellman提出了**公钥密码体制**，并尝试构造公钥密码算法，并用他们的名字命名，称为Diffie-Hellman算法。



Whitfield Diffie

Martin Hellman

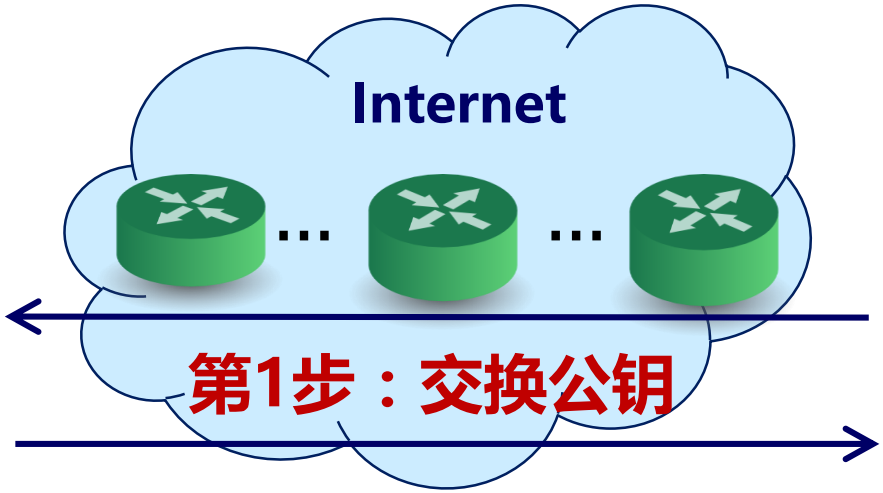
W. Diffie, M. Hellman. *New directions in cryptography*. IEEE Transactions on Information Theory, 1976, No. 6, Vol. 22, 644-654.

Diffie-Hellman公钥密码思想

D-H协议的核心思想

Alice

公钥 K_P^A



第2步：计算共享密钥

$$K = f(K_S^A, K_P^B) \longleftrightarrow K = f(K_S^B, K_P^A)$$

Bob

公钥 K_P^B

1.3 理论基础——单向函数

定义1：令函数f是集A到集B的映射，用 $f: A \to B$ 表示。若对于任意 $x1 \neq x2$，$x1, x2 \in A$，有 $f(x1) \neq f(x2)$，则称 f 为单射，或1-1映射，或可逆的函数。

定义2：一个可逆函数 $f: A \to B$，若它满足：

(1) 对所有 $x \in A$，易于计算 $f(x)$；

(2) 对“几乎所有 $x \in A$”，由 $f(x)$ 求 x 极为困难，以至于几乎是不可能的，则称 f 是一个单向函数。

注意：定义中的“极为困难”是相对现有的计算机资源和算法而言。

1.4 理论基础——陷门单向函数

定义3：陷门单向函数是一类满足下述条件的单向函数：

$f_z: A_z \to B_z$，$z \in Z$，Z是陷门信息集合。

（1）对所有 $z \in Z$，在给定 z 下容易找到一对算法 E_z 和 D_z，使对所有$x \in A$，易于计算 f_z 及其逆，即：

$$f_z(x) = E_z(x)$$

$$D_z(f_z(x)) = x$$

（2）对所有$z \in Z$，当只给定 E_z 和 D_z 时，对所有 $x \in A$，很难从 $y=f_z(x)$计算出 x 。

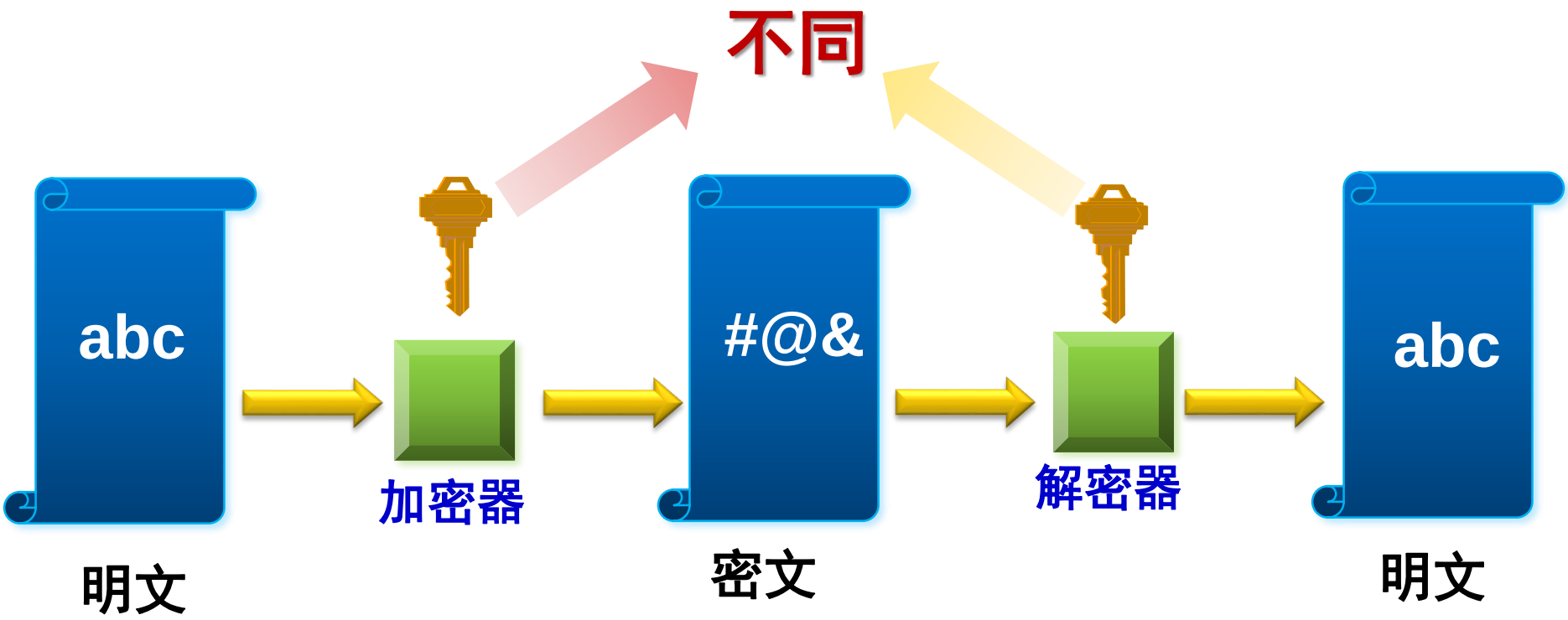
区别：单向函数是求逆困难的函数，而陷门单向函数是在不知道陷门信息下求逆困难的函数。当知道陷门信息后，求逆易于实现。

1.5 用于构造双钥密码的单向函数

- 多项式求根
- 离散对数DL (Discrete Logarithm)
- 大整数分解FAC (Factorization Problem)
- 背包问题 (Knapsack problem)
- Diffie-Hellman问题DHP
- 二次剩余问题QR (Quadratic Residue)
- 模n的平方根问题 (SQROOT)

1.6 公钥密码体制的原理

- 公钥密码，又称非对称密码或双钥密码(Public-key / Two-key/Asymmetric)，其加密和解密数据使用不同的密钥。



1.7 公钥密钥体制的密钥管理

- 公钥密钥体制解决了密钥的发布和管理问题
- 通信双方可以公开其公开密钥，而保留私钥

- 发方可以用收方公钥对发送的信息进行加密
- 收方用自己的私钥对收到的密文进行解密

1.8 公钥密码体制的特点

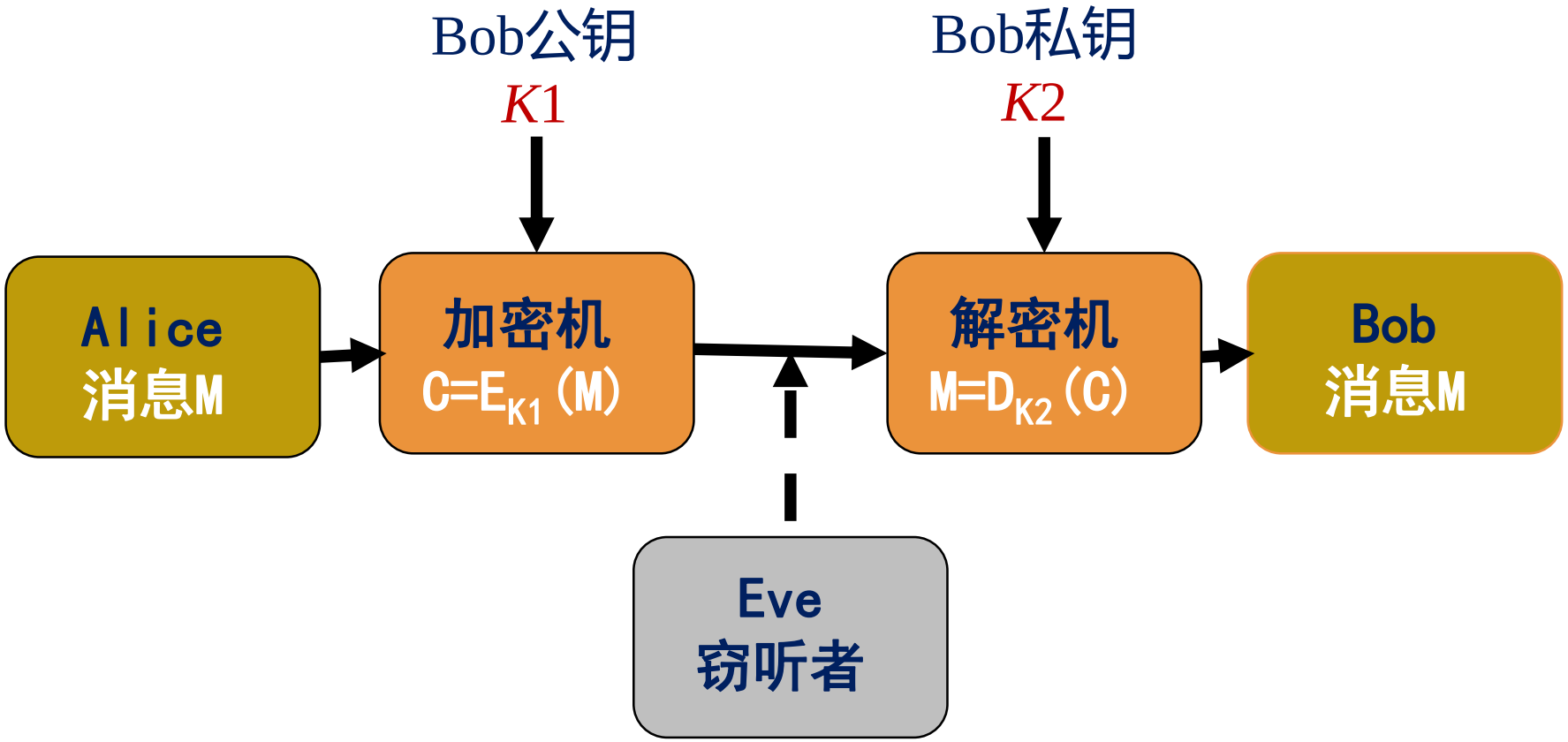
- 每个用户都拥有两个密钥：

公钥(public-key)：可以被任何人知道，用于加密或验证签名

私钥(private-key)：只能由持有者知道，用于解密或签名

- 由私钥及其他密码信息容易计算出公开密钥
- 而由公钥及算法描述，计算私钥却非常困难。

1.9 公钥加密方案



注意：当Alice给Bob发信息时，她必须采用Bob的公钥*K*1对消息加密，而不是采用Alice的公钥对消息加密。Bob采用自己的私钥*K*2对密文解密。这是同学们最容易搞混的地方。

1.9 公钥加密方案

公钥（双钥）密码体制

公钥 K_P^A

公钥 K_P^B

Alice

Bob

$E_{K_P^B}(K_1)$ 第1步：传递会话密钥

$E_{K_1}(m_1)$ 第2步：消息加密传输

第1步：传递会话密钥 $E_{K_P^A}(K_2)$

第2步：消息加密传输 $E_{K_2}(m_2)$

私钥 K_S^A

私钥 K_S^B

1.10 公钥算法的用途

用于密钥分发

- 用于交换秘密信息，
- 常用于交换对称加密密钥

用于消息加密

- 用于对消息直接加密
- 用公钥加密，用私钥解密
- 公钥加密能够用于密钥分配

用于数字签名

- 用用户私钥对消息进行签名
- 接收方用公钥对签名进行验证

1.11 公钥的安全性

- ✓ 安全性依赖于解数学上的困难问题。
- ✓ 穷搜索（exhaustive search）在理论上能够破解公钥密码，当密钥足够长 时，破解极其困难。
- ✓ 目前，通常要求足够大的密钥长度 (>1024 bits)
- ✓ 密钥太长会导致加密速度缓慢，因此公钥算法仅用于密钥传递，而不用于实时的数据加密。

双钥密码体制（一）

一 公钥密码体制的基本概念

二 RSA公钥密码算法

三 ElGamal公钥签名算法

四 其它公钥密码

二、RSA公钥密码算法

RSA算法, 于1978由Rivest, Shamir, Adleman三人共同提出。

2.1 RSA公钥算法说明

- Rivest, Shamir和Adleman 于1977年研制并且1978年首次公开发表。
- RSA是一种分组密码，其理论基础是一种特殊的可逆模指数运算，其安全性基于分解大整数的困难性。
- 既可以用于消息加密，也可用于数字签名。
- 硬件实现时，比DES慢约1000倍。软件实现时比DES慢约100倍。
- 已被许多标准化组织（如ISO、ITU、IETF和SWIFT等)接纳，目前多使用RSA公司的PKCS系列标准；
- RSA-155（密钥长度512 bit）于1999年分别被分解。

2.1 RSA公钥算法说明

- 设 n 是两个不同奇素数之积，即 $n = p \times q$，计算其欧拉函数值$\varphi(n) = (p-1)(q-1)$。
- 随机选一整数e, $1 < e < \varphi(n)$, $(\varphi(n), e) = 1$

  因而在模 $\varphi(n)$下, e有逆元：$d = e^{-1} \bmod \varphi(n)$

互素

- 取公钥为n, e, 私钥为d (p, q不再需要，可以销毁，但绝不可泄露)
  - ✓ 加密变换为 $m \rightarrow c = m^e \bmod n$
  - ✓ 解密变换为 $c \rightarrow c^d = m \bmod n$

2.2 RSA算法的关键技术

密钥选择

- 模数大于1024bit，p, q为大素数
- p-1，q-1有大的素因子
- p+1，q+1也要有大的素因子
- e不能太小，最常用的 e 值为3，17，65537（$2^{16}+1$）

算法实现

- 可以用软件/硬件实现
- 软件与硬件结合,可采用并行算法

2.3 RSA算法的使用

- 设Bob的公钥为(e, n)，私钥为 d, 明文为m
- Alice用Bob的公钥计算：$c=m^e \mod n$，发给B
- Bob用Bob的私钥计算：$m=c^d \mod n$
- 特点:
  - ✓ 即使A和B从来不认识，都可进行保密通讯，只要知道B的公钥。
  - ✓ 速度慢，它不适用于对图像、话音等进行实时数据加密。
- 要求对公开密钥进行保护，防止修改和替换。

2.4 RSA算法的举例说明

1. 选p_1=47, p_2=71, 则n=47×71=3337, φ(n)=46×70=3220。若选e=79，可计算$d=e^{-1}(\mathrm{mod}\ 3220)=1019$
2. 公开钥n=3337和e=79，秘密钥d=1019。销毁p_1和p_2。
3. 另明文为x=688 232 687 966 668 3，分组得x_1=688, x_2=232, x_3=687, x_4=966, x_5=668, x_6=3
4. 对x_1加密为：$(688)^{79} \mathrm{mod}\ 3337=1570=C_1$
5. 同样可计算出其它各组密文：y=1570 2756 2714 2423 158
6. 对C_1解密：$(1570)^{1019} \mathrm{mod}\ 3337=668=x_1$

   类似地可解出其它各组密文，恢复出明文。

2.5 RSA算法的安全性

密钥长（bit）	所需MIPS年
116	400
129	5000
512	30000
768	200 000 000
1024	300 000 000 000
2048	300 000 000 000 000

2.6 等价密钥长度——与单钥体制比较

单钥体制	RSA体制	单钥体制	RSA体制
56 b	384 b	112 b	1792 b
64 b	512 b	128 b	2304 b
80 b	768 b		

双钥密码体制（一）

一 公钥密码体制的基本概念

二 RSA公钥密码算法

三 **ElGamal公钥签名算法**

四 其它公钥密码

三、ElGamal公钥算法

ElGamal于1985年基于离散对数问题提出了一个既可用于数字签名又可用于加密的密码体制；(此数字签名方案的一个修改被NIST采纳为数字签名标准DSS)

ElGamal,Schnorr和DSA签名算法都非常类似。事实上，它们仅仅是基于离散对数问题的一般数字签名的三个例子。

ElGamal方案未申请专利。但受到DH专利的制约（DH专利已经在1997年4月29日到期）。

3.1 ElGamal公钥密码算法

ElGamal公钥加密算法, 1985

- 其安全性依赖于离散对数问题（**discrete logarithms problem**）
- 参数： **GF(*p*)**上的本原元***g***
- 秘密钥： ***x*** in **GF(*p*)*** （**except 0**）
- 公钥：$y=g^x \bmod p$
- 选择一个随机数：***k***
- encryption: $m \to (g^k, my^k) \bmod p = (r, s)$
- decryption: $m = sr^{-x} \bmod p$

专题：双钥密码体制（一）

一 公钥密码体制的基本概念

二 RSA公钥密码算法

三 ElGamal公钥签名算法

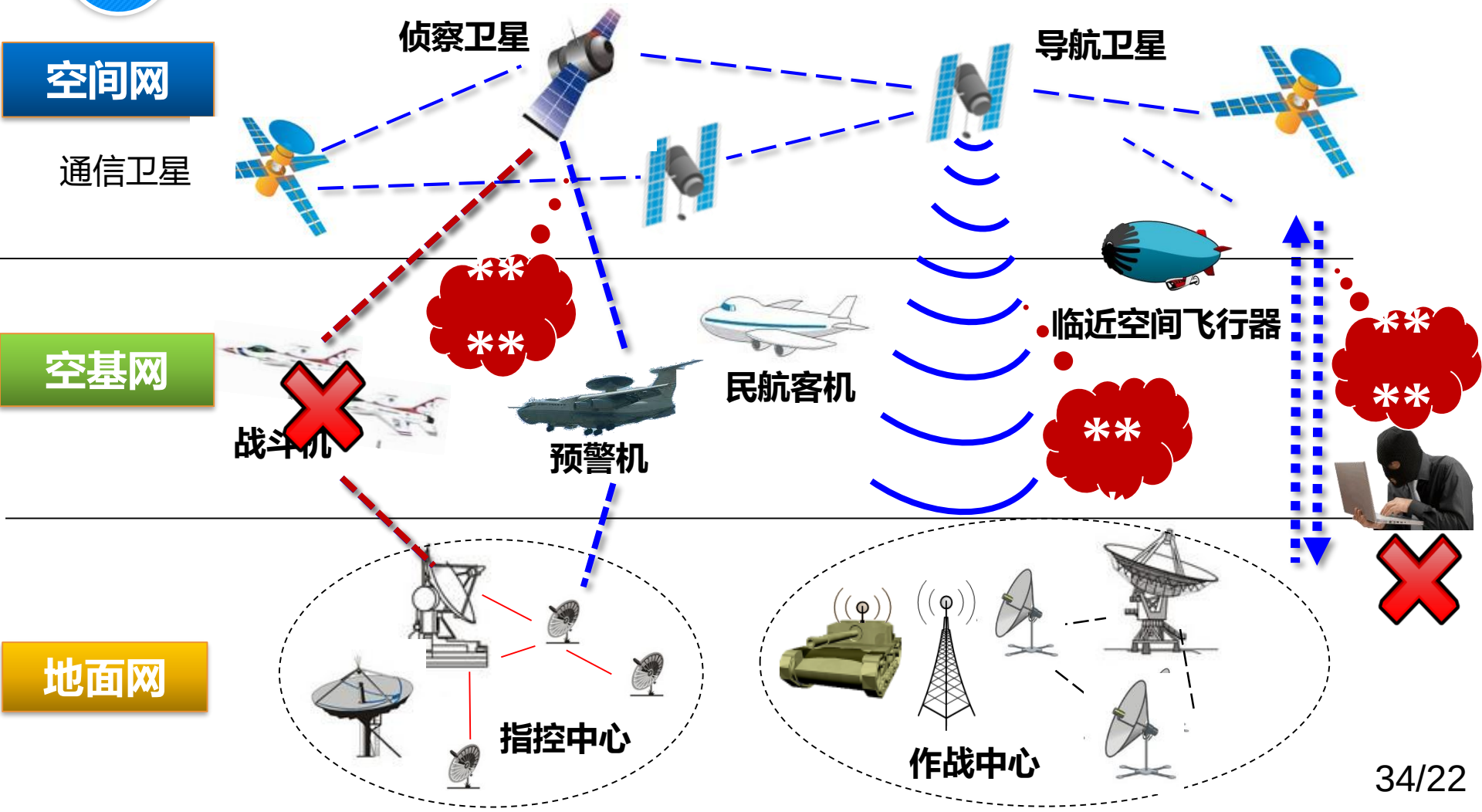
四 其它公钥密码

四、其它公钥密码

1. Rabin密码体制，是RSA的一个特例。
2. 背包密码体制。
3. McEliece 体制。1978年，提出了一种基于纠错编码的公开钥密码系统，该系统使用了一类Goppa纠错码。
4. LUC密码体制。新西兰学者Smith提出。
5. 1985年，Neal Koblitz和V.S.Miller将椭圆曲线（ECC）用于公开钥密码，并用椭圆曲线实现了DH算法。
6. 有限自动机体制。中国学者陶仁骥等提出。
7. 概率加密体制。

公钥密码体制的应用

空间网络密钥的自动分发和更新



谢谢！