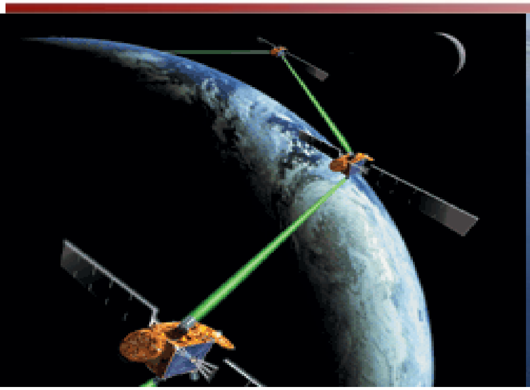
普通高等教育“十一五”国家级规划教材

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18日

双钥密码体制（二）

一　Diffie-Hellman公钥密码体制

二　Rabin公钥密码体制

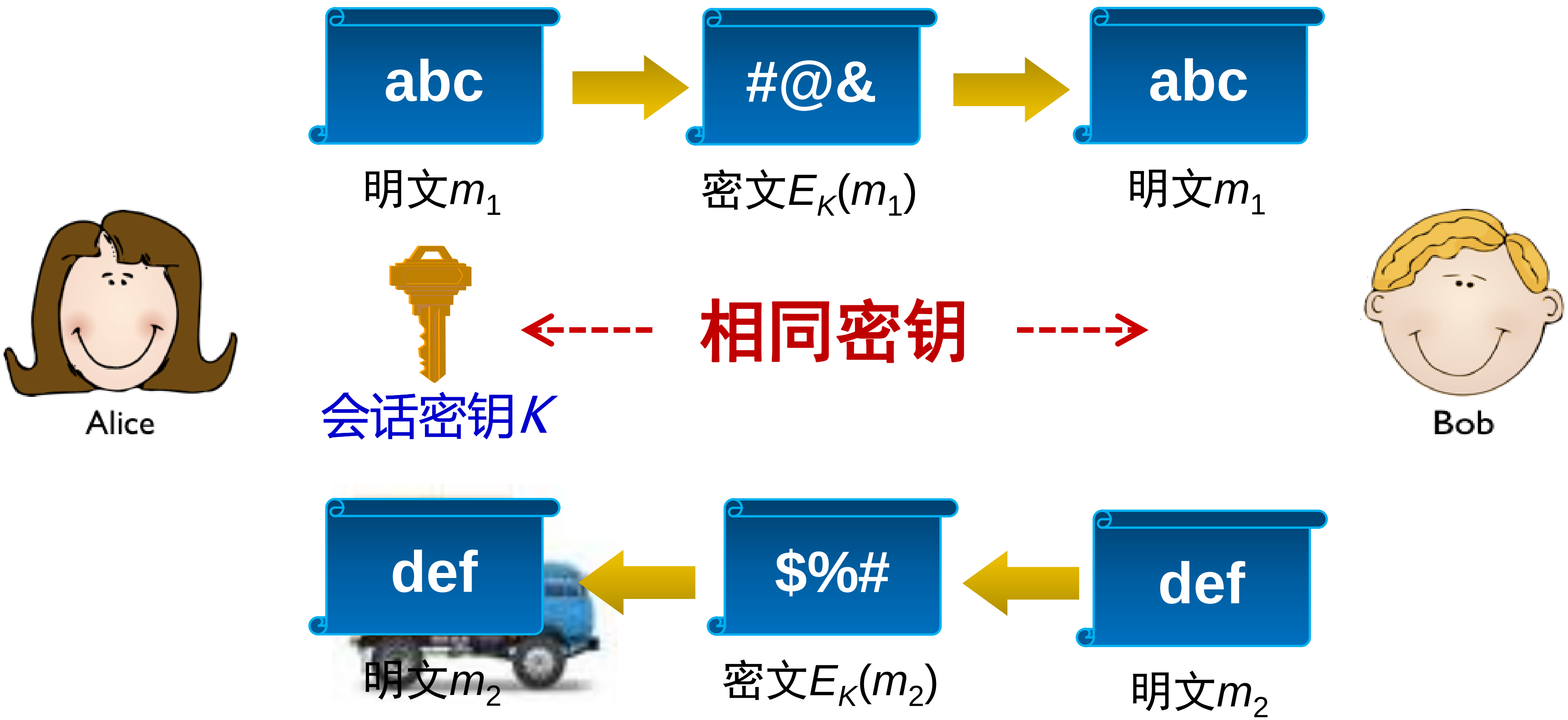
三　椭圆曲线公钥密码体制

双钥密码体制（二）

- 一 Diffie-Hellman公钥密码体制
- 二 Rabin公钥密码体制
- 三 椭圆曲线公钥密码体制

一、 Diffie-Hellman公钥密码体制

回顾：对称（单钥）密码体制

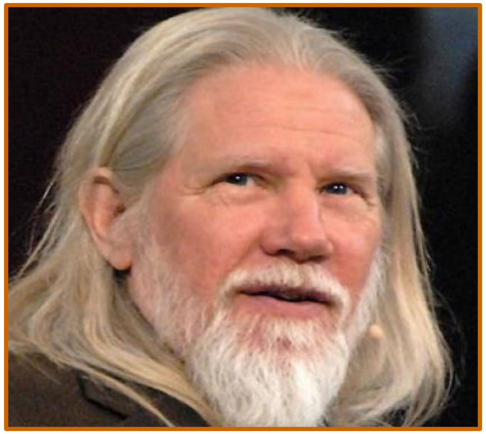


一、 Diffie-Hellman公钥密码体制

D-H协议简介——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。

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

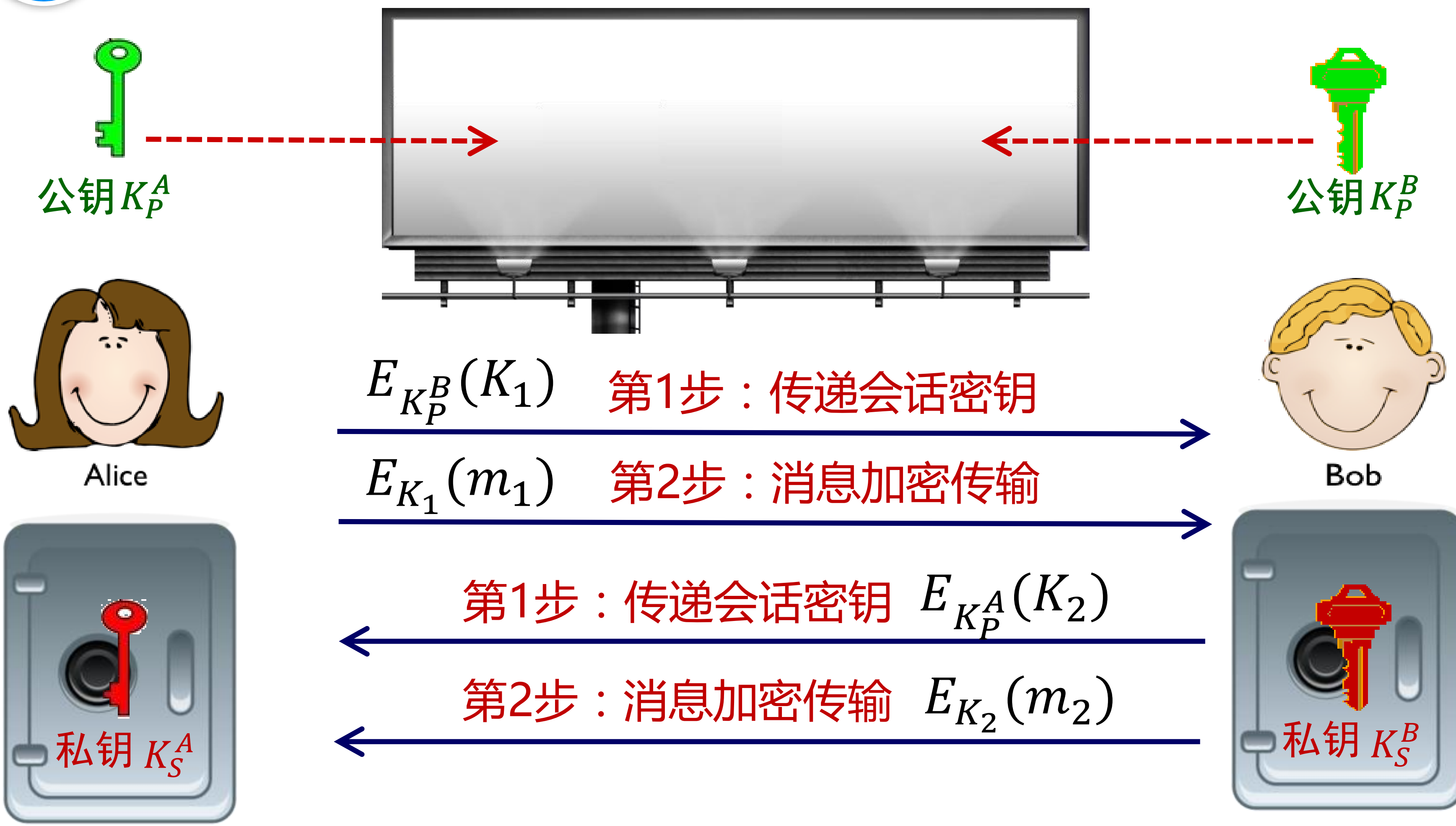


Whitfield Diffie

Martin Hellman

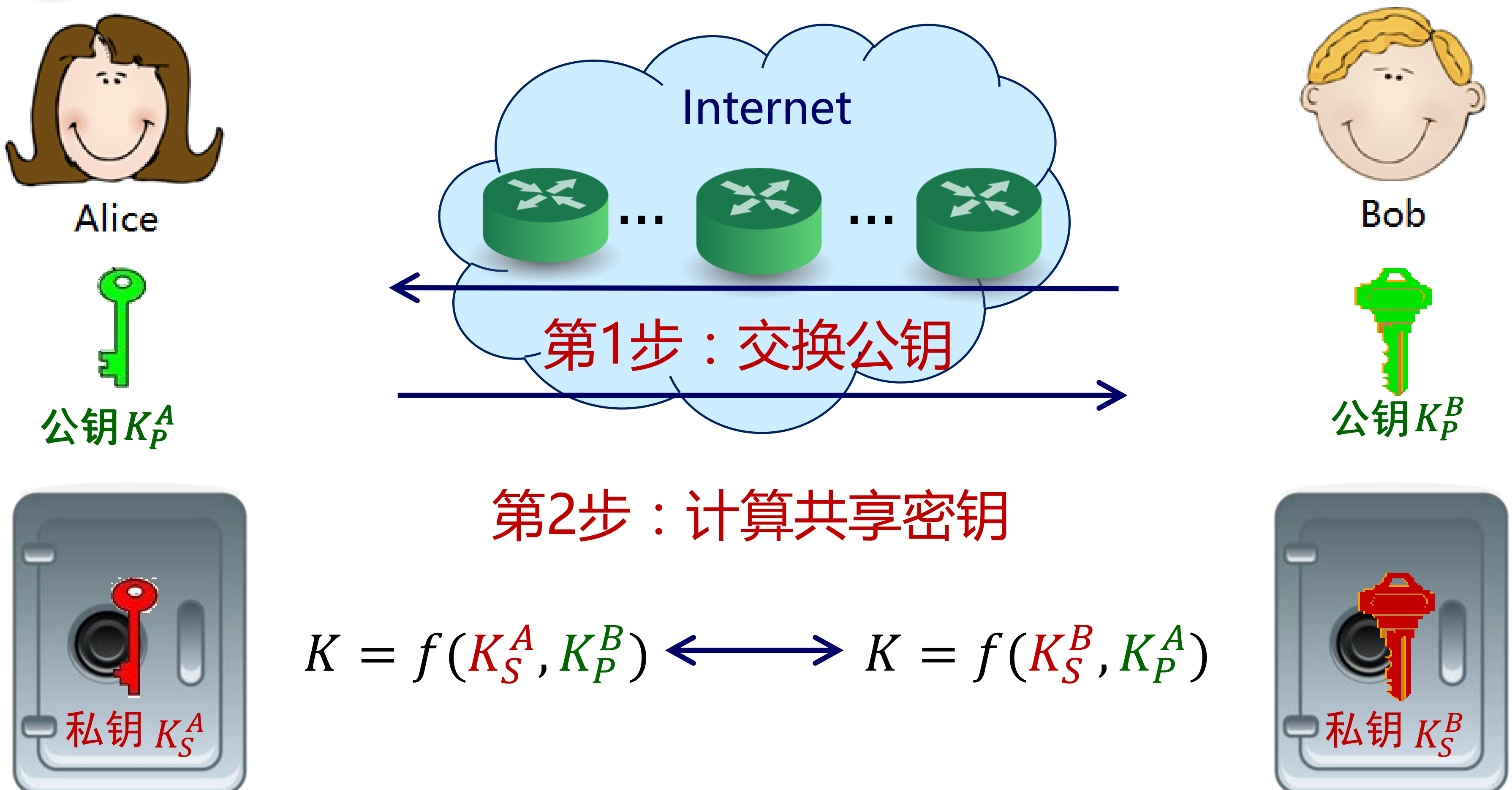
一、 Diffie-Hellman公钥密码体制

回顾：公钥（双钥）密码体制



一、 Diffie-Hellman公钥密码体制

D-H协议的核心思想



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

一、 Diffie-Hellman公钥密码体制

D-H协议基于求解离散对数难题

常用于构造公钥密码体制的数学难题：

- **【离散对数问题】**
- 【多项式求根问题】
- 【大整数分解问题】
- 【背包问题】
- 【Diffie-Hellman问题】
- 【二次剩余问题】
- 【模n的平方根问题】

实数域中计算：

$$y = g^x$$ 容易

$$x = log_g y$$ 容易

有限域中计算：

$$y = g^x \bmod p$$ 容易

$$x = dlog_{g,p} y \bmod p$$ 困难!

一、 Diffie-Hellman公钥密码体制

什么是离散对数问题？

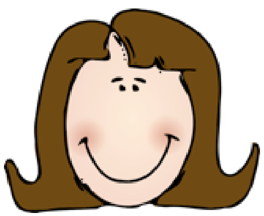
给定一个大素数p，可构造一个$(p-1)$阶循环群Z_p^*，在此群上必有一个本原元g $(1 < g < p-1)$。

若已知x，容易求$y = g^x \bmod p$，只需$\lfloor lb2x \rfloor - 1$次乘法。
例如：$x = (15)_{10} = 1111_2$，$g^{15} = (((1 \cdot g)^2 \cdot g)^2 \cdot g)^2 \cdot g \bmod p$，只需用6次乘法。

若已知y, g, p，求$x = dlog_{g,p} y \bmod p$为离散对数(Discrete Logarithm)问题，最快求解法的运算次数渐近值为：$L(p) = O(\exp\{(1+o(1))\sqrt{\ln p \cdot \ln(\ln p)}\})$。
例如：当$p = 512$时，$L(p) = 2^{256} \approx 10^{77}$。

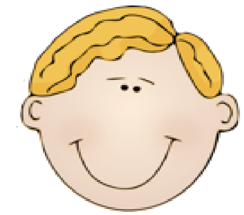
一、 Diffie-Hellman公钥密码体制

D-H协议的具体过程——密钥交换过程



Alice

约定：Alice和Bob均知道两个大素数p和g，其中g是群$Z_p=\{0,\ldots,p-1\}$上的本原元。大素数p和g是公钥，是可以公开的参数。



Bob

Alice选择私钥$X_A<p$

Bob选择私钥$X_B<p$

Alice计算公钥$Y_A=g^{X_A} \bmod p$

Bob计算公钥$Y_B=g^{X_B} \bmod p$

Alice收到Bob的公钥Y_B

Bob收到Alice的公钥Y_A

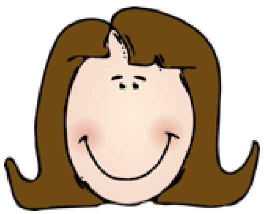
Alice 计 算 共 享 密 钥 $K=Y_B^{X_A} \bmod p=g^{X_AX_B} \bmod p$

=

Bob 计 算 共 享 密 钥 $K=Y_A^{X_B} \bmod p=g^{X_AX_B} \bmod p$

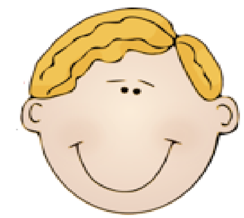
一、Diffie-Hellman公钥密码体制

D-H协议的具体过程——举例



Alice

令两个大素数$p=97$和$g=5$，其中g是群$(0,\ldots,96)$上的本原元。这两个整数公开，可以通过不安全信道传输它们。



Bob

① Alice选择私钥$X_A=36$，计算公钥$Y_A=5^{36} \bmod 97=50$

② Bob选择私钥$X_B=58$，计算公钥$Y_B=5^{58} \bmod 97=44$

③ Alice计算

$$K=44^{36} \bmod 97=75$$

$=$

④ Bob计算

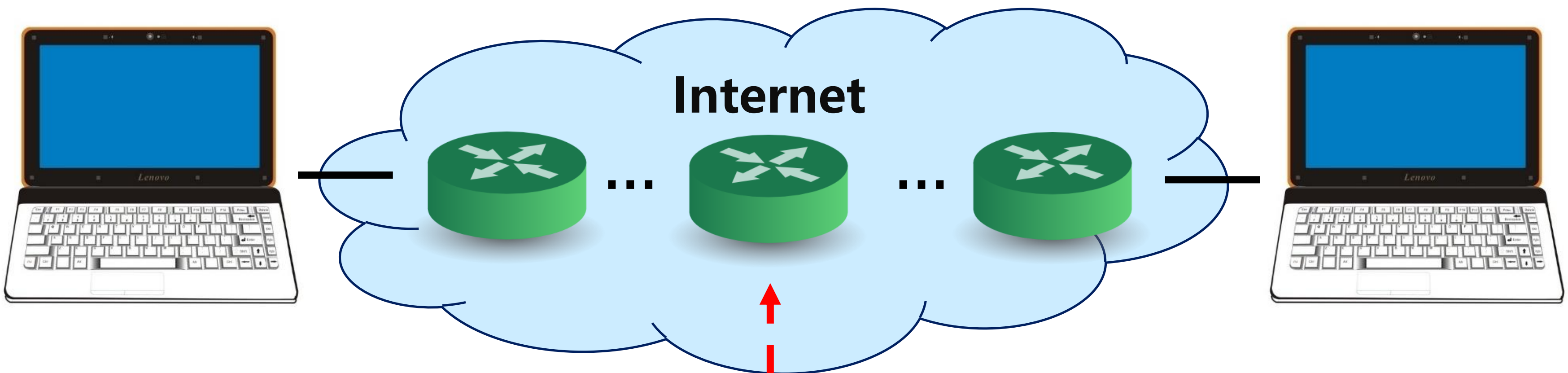
$$K=50^{58} \bmod 97=75$$

一、 Diffie-Hellman公钥密码体制

提问：D-H协议有何安全问题？

一、 Diffie-Hellman公钥密码体制

D-H协议的安全性——不能抵抗中间人攻击



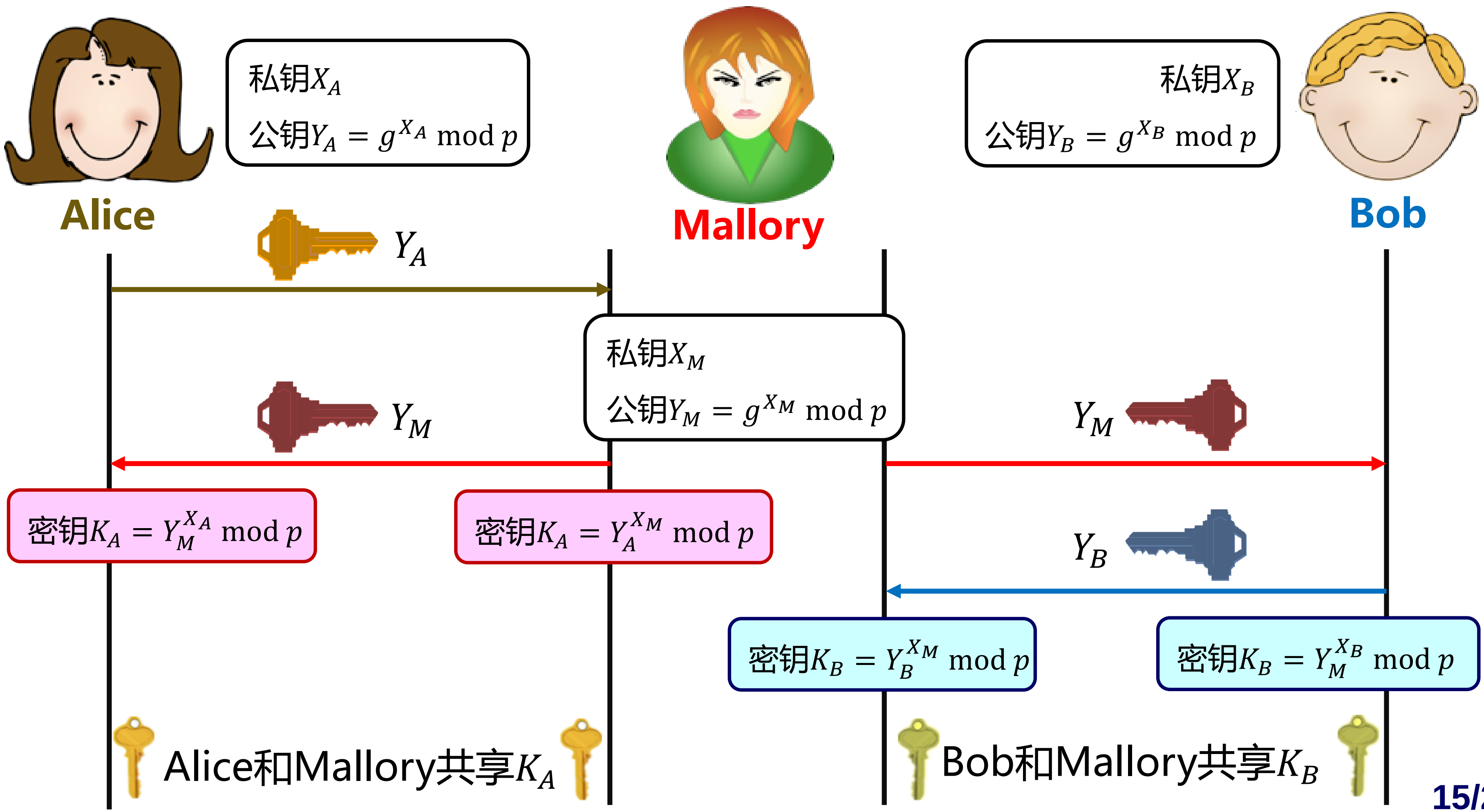
中间人攻击：

通过拦截正常的网络通信数据，对通信内容进行嗅探和篡改，在这一过程中，正常通信的双方往往毫不知情。

D-H协议不能抵抗中间人攻击!

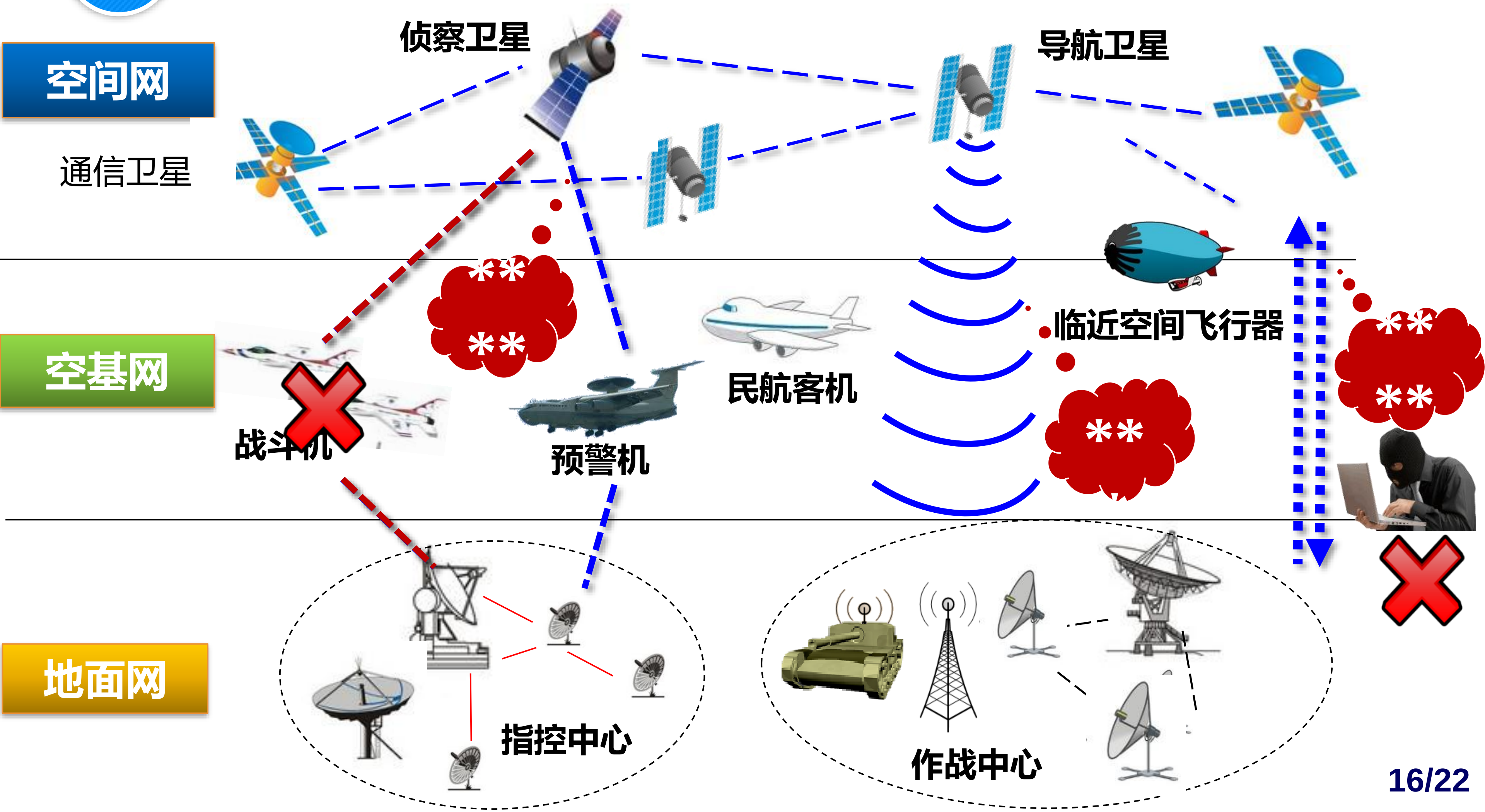
一、 Diffie-Hellman公钥密码体制

D-H协议的安全性——中间人攻击过程



一、 Diffie-Hellman公钥密码体制

D-H协议应用：空间网络密钥的自动分发和更新



Diffie-Hellman 应用的问题

一 两个主体每次可以选择新的秘密钥(私钥)，并计算及交换新的公钥

二 可以抵抗被动攻击，但不能抵抗中间人攻击

三 为抵抗中间人攻击，需要改进此协议

双钥密码体制（二）

一 Diffie-Hellman公钥密码体制

二 Rabin公钥密码体制

三 椭圆曲线公钥密码体制

二、Rabin公钥密码体制

- 1979年，Rabin利用合数模下求解平方根的困难性构造了一种安全的公钥体制。
- Rabin公钥体制已经被证明：对该体制的破译的难度等价于大整数分解。
- Rabin体制是RSA的一种特例，它有以下两个特点：
  - 它不是以一一对应的单向陷门函数为基础，即对于同一密文，可能对应有两个以上的明文。
  - 破译该体制等价于大整数的分解。
- RSA中选取的公开钥e满足$1 < e < \varphi(n)$，且$\gcd(e, \varphi(n))=1$。而Rabin体制则选择$e=2$。

2.1 密钥的产生

1. Rabin体制则选择e=2

2. 随机选择两大素数p, q

满足$p≡q≡3 \bmod 4$ 即这两个素数的形式为：$4k+3$（k为整数）

3. 计算：$n=p \times q$

4. n, e作为公钥

5. p, q为私钥

2.2 Rabin加密过程

- 假设B要将消息加密后发给A；
- A公布其公开钥：n, e=2
- B将明文分组为m_1,m_2,m_3,m_4……。设其中一个明文分组为消息m
- B计算密文：$c \equiv m^e \equiv m^2 \bmod n$
- B将密文c发给A。

2.3 Rabin解密过程

- A解密，就是求c的模n平方根，即解$x^2 \equiv c \bmod n$；
- 由中国剩余定理可知，解以上方程等价于解方程组：

$$\begin{cases} x^2 \equiv c \bmod p \\ x^2 \equiv c \bmod q \end{cases}$$

- 由于$p \equiv q \equiv 3 \bmod 4$，可以很容易求出方程组的解：

$$x \equiv m \bmod p \qquad x \equiv -m \bmod p$$
$$x \equiv m \bmod q \qquad x \equiv -m \bmod q$$

- 经过组合可以得到4个同余方程组：

2.3 Rabin解密过程（续）

$$\begin{cases} x \equiv m \bmod p \\ x \equiv m \bmod q \end{cases} \qquad \begin{cases} x \equiv m \bmod p \\ x \equiv -m \bmod q \end{cases}$$

$$\begin{cases} x \equiv -m \bmod p \\ x \equiv m \bmod q \end{cases} \qquad \begin{cases} x \equiv -m \bmod p \\ x \equiv -m \bmod q \end{cases}$$

- 可见：由中国剩余定理解出的每一方程组的解有4个，即每一密文对应的明文不是唯一的。

解决办法：为了有效地确定唯一的明文，发送者可以在明文消息m中加入某些信息，如发送者的身份号、接收者的身份号、日期、时间等。

双钥密码体制（二）

一 Diffie-Hellman公钥密码体制

二 Rabin公钥密码体制

三 椭圆曲线公钥密码体制

三、椭圆曲线密码体制ECC

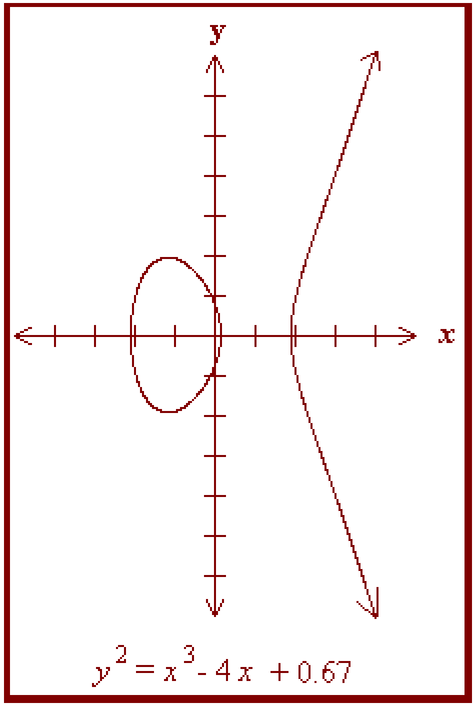
- 1985年，Koblitz和Miller独立将椭圆曲线（Elliptic Curve）引入密码学中，成为构造双钥体制的有力工具。
- 目前，对这种椭圆曲线离散对数密码体制研究已经有20年的历史，尚未发现明显的弱点。
- 目前，大多数的产品和标准均使用RSA。为了保证RSA的安全性，近年来所采用的密钥长度不断增加，这直接导致了RSA计算量的增加。
- ECC对RSA提出了巨大的挑战。在公钥密码的标准化过程中，IEEE P1363标准已经采用了ECC。
- 与RSA相比，ECC的主要优点是可以使用比RSA更短的密钥获得相同水平的安全性。

3.1 实数域上椭圆曲线的概念

- 实数域上的椭圆曲线可以定义为满足方程：$y^2 = x^3 + ax + b$ 的所有点(x, y)的集合

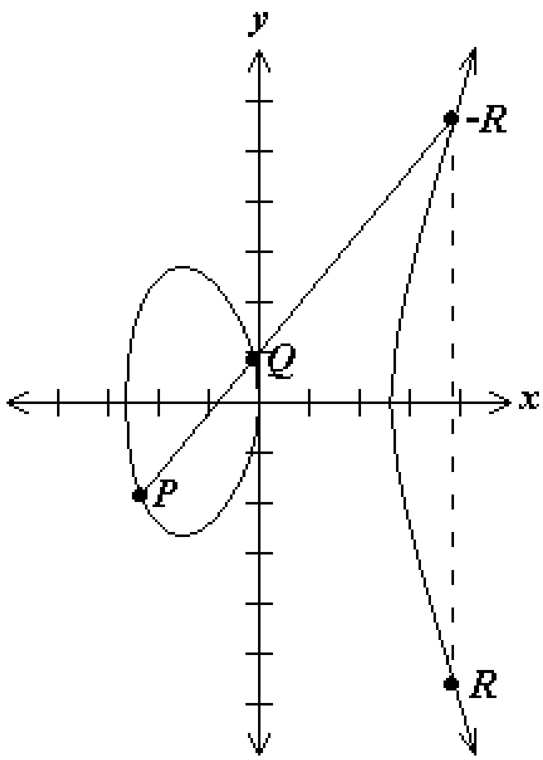
注意：椭圆曲线并不是椭圆，只因为该方程与计算椭圆周长的方程相似。

- 可以证明：如果$x^3 + ax + b$ 没有重复因子，或者满足$4a^3 + 27b^2 \neq 0$ ，那么椭圆曲线上的点集$E(a, b)$可构成一个Abel群。
- 椭圆曲线群包括所有曲线上的点以及一个特殊的点，我们称其为无限远点 O
- 群定义：若在集合上定义的加法运算是封闭的，且满足交换律和结合律，我们就称这个集合为群。



实数域椭圆曲线上加法: P+Q

加法定律：$P + Q = R$



P (-2.35, -1.86)

Q (-0.1, 0.836)

$-R$ (3.89, 5.62)

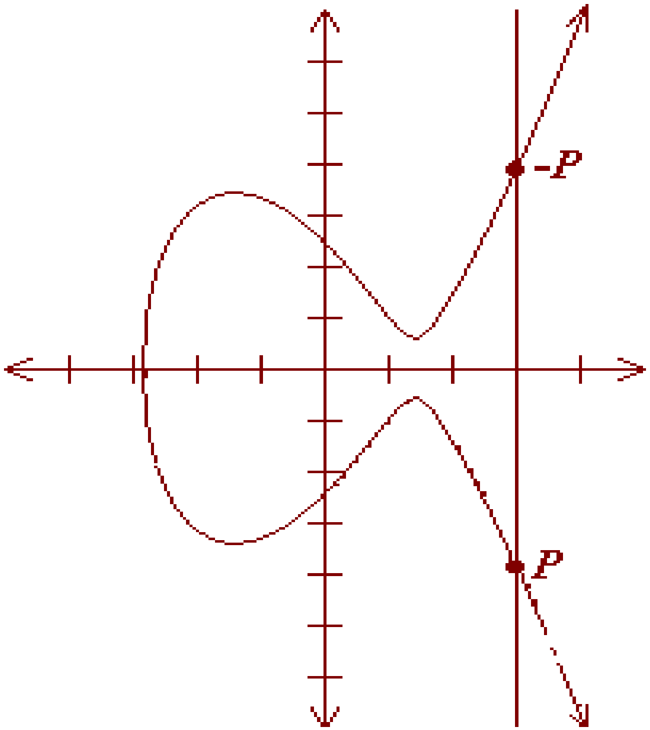
R (3.89, -5.62)

$P + Q = R = (3.89, -5.62).$

$$y^2 = x^3 - 7x$$

实数域椭圆曲线上加法: P+(-P)

加法定律 P + (-P) = O

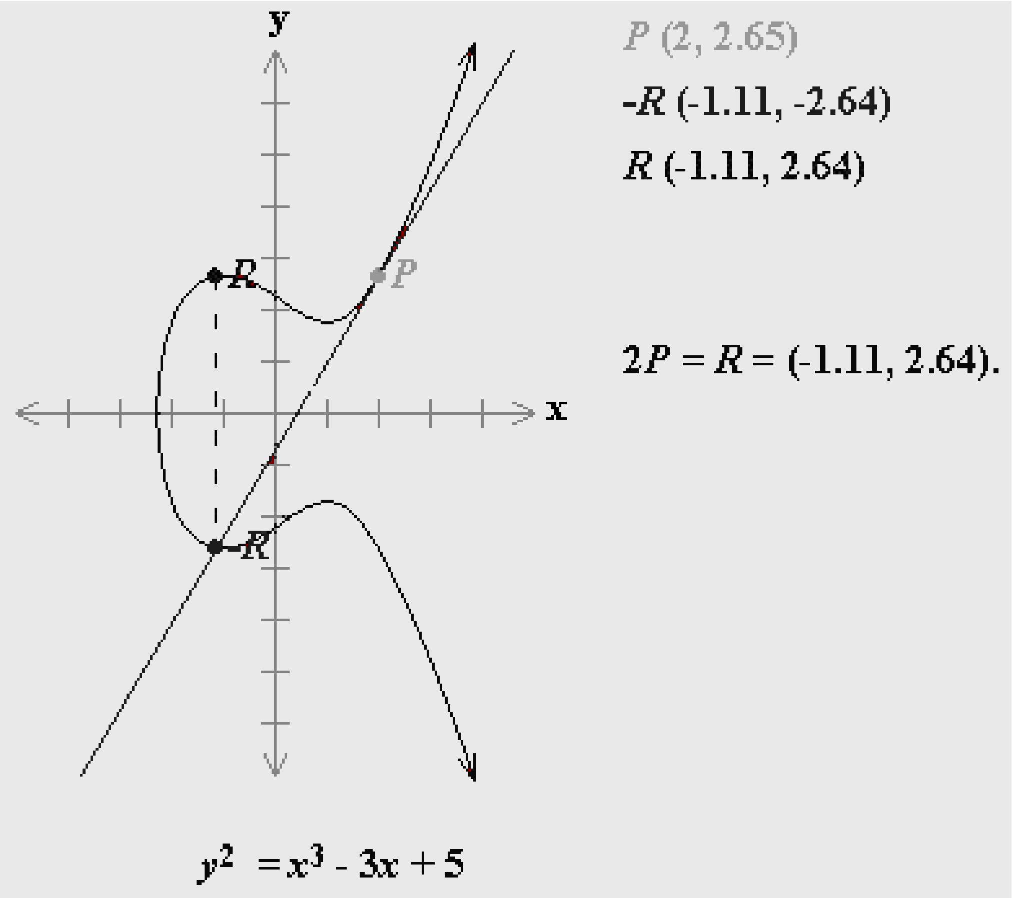


$P + (-P) = O$

$y^2 = x^3 - 6x + 6$

实数域椭圆曲线上加法：2P

加法定律：**2P= P +P = R**



3.2 有限域$E_p(a, b)$上的椭圆曲线

- 有限域 F_q 上的椭圆曲线$y^2 = x^3 + ax + b$，其点集(x, y)构成有限域上的Abel群，记为$E_p(a, b)$。条件为：

$4a^3 + 27b^2 \neq 0 \bmod q$

设$P=(x_1, y_1)$, $Q=(x_2, y_2)$, $P+Q=(x_3, y_3)$

- 那么，当$P \neq Q$ 时：

$$\lambda = \left(\frac{y_2 - y_1}{x_2 - x_1}\right) \bmod q$$

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod q$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod q$$

3.2 有限域$E_p(a, b)$上的椭圆曲线

当$P = Q$时：

$$\lambda = (\frac{3x_1^2 + a}{2y_1}) \bmod q$$

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod q$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod q$$

举例说明—$E_{23}(1,1)$的椭圆曲线

- 取$p=23$, $a=b=1$, 则椭圆曲线方程为：$y^2=x^3+x+1 \bmod p$
- 把满足上式的所有点(x, y)和元素O所组成的点集记为$E_{23}(1,1)$
- 对于$E_{23}(1, 1)$，只关心满足模 p 方程的、从$(0, 0)$到 $(p-1, p-1)$的象限中的非负整数。下表列出$E_{23}(1, 1)$若干点(O 点除外)。

(0, 1)	(6, 4)	(12, 19)
(0, 22)	(6, 19)	(13, 7)
(1, 7)	(7, 11)	(13, 16)
(1, 16)	(7, 12)	(17, 3)
(3, 10)	**(9, 7)**	(17, 20)
(3, 13)	(9, 16)	(18, 3)
(4, 0)	(11, 2)	(18, 20)
(5, 4)	(11, 20)	(19, 5)
(5, 19)	(12, 4)	(19, 18)

(9,7)

举例说明——$E_{23}(1,1)$的椭圆曲线

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \quad (1)$$

系数满足： $4a^3 + 27b^2 \neq 0 \bmod p \quad (2)$

说明：对于有限域Fp上的椭圆曲线，使用变元和系数均在0到p-1的整数集上取值的三次方程，其中p是大素数，所执行的运算均为模p运算。

- 例如：当a=1, b=1, p=23时可满足(2)式：

  $4\times1^3+27\times1^2=31 \bmod 23\neq0$

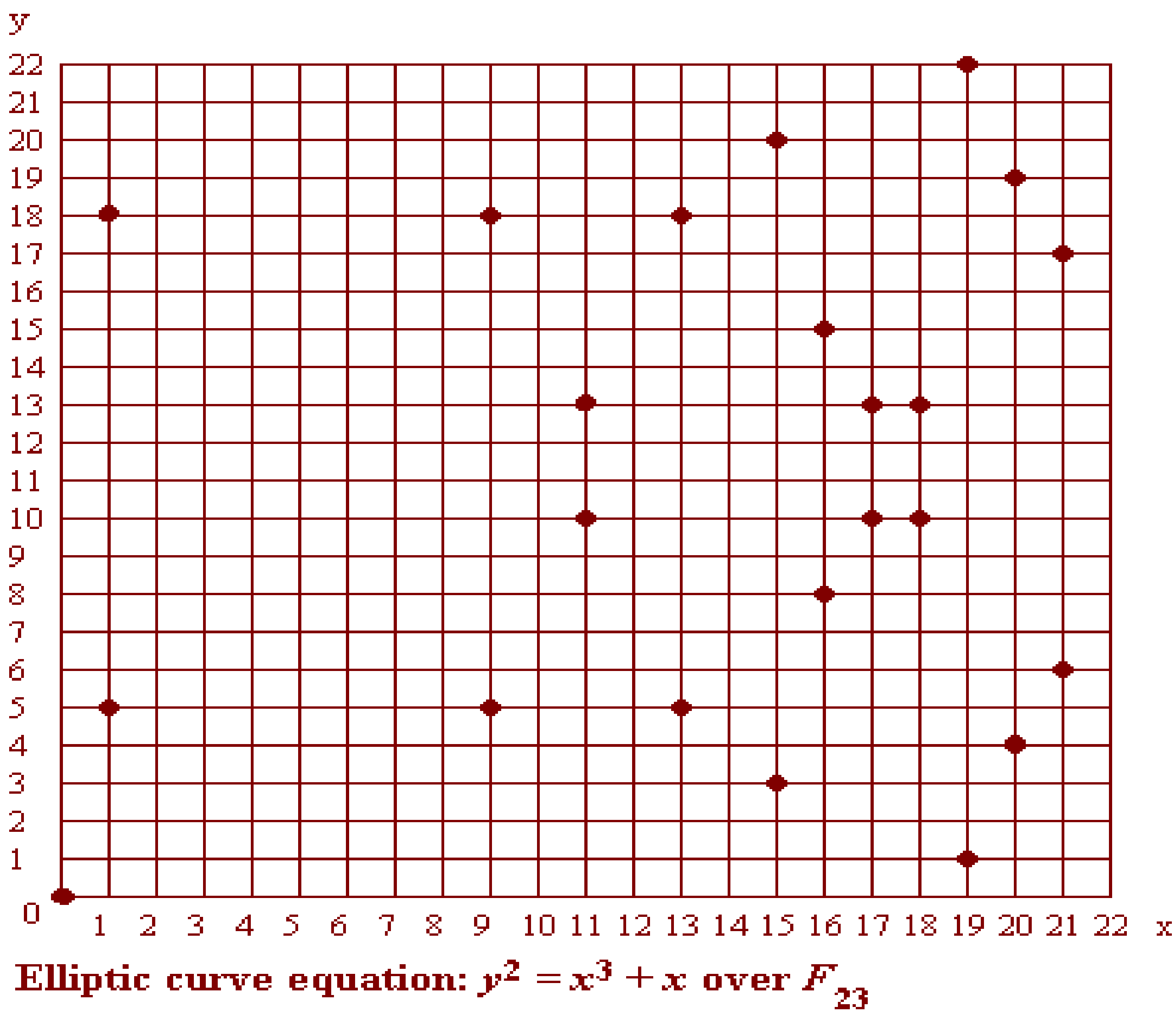
- 且x=9, y=7时，(1)式的两边分别为：

$$7^2 \bmod 23 = (9^3 + 9 + 1) \bmod 23$$

$$49 \bmod 23 = 739 \bmod 23$$

$$3 \bmod 23 = 3 \bmod 23$$

举例说明—$E_{23}(1,1)$的椭圆曲线



举例说明—E_{23}的椭圆曲线

例如：$E_{23}(1, 1)$为一椭圆曲线，设P=(3,10), Q=(9,7)，则：

$$\lambda = \left(\frac{y_2 - y_1}{x_2 - x_1}\right) \bmod q$$

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod q$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod q$$

可以求出： $x_3 = 11^2\text{-}3\text{-}9 = 109 = 17 \bmod 23$

$y_3 = 11\cdot (3\text{-}17)\text{-}10 = \text{-}164=20 \bmod 23$

所以： P+Q=(17, 20)

可以看出，P+Q仍然为椭圆曲线$E_{23}(1,1)$上的点。

举例说明—$E_{23}(1,1)$的椭圆曲线

设P=(3,10)，则2P的计算为：

$$\lambda = \left(\frac{3x_1^2 + a}{2y_1}\right) \bmod q$$

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod q$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod q$$

可以求出：　$x_3=6^2-3-3=30=7 \bmod 23$

$y_3=6\,(3-7)-10=-34=12 \bmod 23$

所以：　2P=(7, 12)

可以看出：2P仍然为椭圆曲线$E_{23}(1,1)$上的点。

同理，我们可以求出：4P=P+P+P+P

结　论

- 从上例可以看出：加法运算在$E_{23}(1, 1)$上是封闭的，且还能验证满足交换律。

- 对于一般形式的$E_p(a, b)$，可证明其上的加法运算是封闭的，且满足交换律。

- 同样，我们还可以证明$E_p(a, b)$上的加法逆元运算也是封闭的。

- 根据群的定义可知，$E_p(a, b)$是一个Abel群。

3.3 建立在椭圆曲线上的密码

- 为了使用 椭圆曲线构造公钥密码体制，需要找出椭圆曲线上的数学难题。

在椭圆曲线构成的Abel群$E_p(a, b)$上，考虑方程：**Q=*k* P**，

其中P, Q$\in E_p(a, b)$, $k < p$

由 k 和 P 计算 Q 非常容易；

而由P, Q 计算 k 则非常困难。

这就是椭圆曲线上的离散对数问题—ECDLP

- 由于Diffie-Hellman以及ElGamal是基于有限域上的离散对数问题构造的公钥体制，因此我们也可以采用椭圆曲线来构造它们。

椭圆曲线上的Diffie-Hellman密钥交换

- 首先取一素数$p≈2^{180}$，以及参数a, b，则椭圆曲线上的点构成Abel群$E_p(a, b)$。
- 取$E_p(a, b)$上的一个生成元G (x_1, y_1)，要求G的阶是一个非常大的数n，G的阶n是满足$nG=O$的最小正整数。
- 将$E_p(a, b)$和生成元G作为公钥密码体制的公开参数对外公布，不保密。

EC上的Diffie-Hellman密钥交换算法

- A选择一小于n的整数n_A作为私钥，由$P_A=n_AG$产生E_p(a,b)上的一点作为公钥。
- B选取自己的私钥n_B，并计算自己的公钥$P_B=n_BG$。
- A可以获得B的公钥P_B
- B可以获得A的公钥P_A
- A计算：$K=n_A\times P_B= n_An_BG$
- B计算：$K=n_B\times P_A= n_An_BG$

至此，A和B共同拥有密钥$K= n_An_BG$。攻击者如果想获得密钥K，他就必须由P_A和G求出n_A，或者由P_B和G求出n_B，而这等价于求椭圆曲线上的离散对数问题ECDLP，因此是不可行的。

举例说明—EC上的DH密钥交换算法

- 选择p=211，$E_{211}(0, -4)$，即椭圆曲线为$y^2 \equiv x^3 - 4 \bmod 211$
- $G=(2, 2)$是$E_{211}(0, -4)$上的一个生成元，阶n=241，$241G=O$
- A取私钥为$n_A=121$，可计算公钥$P_A=121\times(2, 2)=(115, 48)$
- B取私钥为$n_B=203$，可计算公钥$P_B=203\times(2, 2)=(130, 203)$
- A计算共享密钥：$121\times P_B=121\times(130, 203)=(161, 169)$
- B计算共享密钥：$203\times P_A=203\times(115, 48)=(161, 169)$

可见，此时A和B共享密钥是一对数据 **(161, 169)**。
如果在后续采用单钥体制加密时，可以简单地取其中的一个坐标，比如x坐标161，或x坐标的一个简单函数作为共享的密钥进行加密/解密运算。

椭圆曲线公钥加密/解密算法

准备阶段：

- A选择一小于n的整数n_A作为私钥，由$P_A=n_A G$产生$E_p(a, b)$上的一点作为公钥。
- B选取自己的私钥n_B，并计算自己的公钥$P_B=n_B G$。

加密阶段：

- 若A要将消息m加密后发给B，则A选择一个随机数k，计算：

$$C=\{ kG, m + kP_B \}$$

解密阶段：

- B收到密文C后，则需用第二个点减去第一个点与B的私钥之乘积：

$$m=(m + kP_B) - n_B (kG)= \mathrm{m} + k (n_B G) - n_B (kG)$$

举例说明—EC上的加密/解密算法

- 选择p=257，$E_{257}(0, -4)$，即椭圆曲线为$y^2 \equiv x^3 - 4 \bmod 257$
- $G=(2, 2)$是$E_{257}(0, -4)$上的一个生成元
- Bob取私钥为$n_B=101$，可计算公钥$P_B=101\ (2, 2)=(197, 167)$
- Alice欲将明文$m=(112, 26)$加密发送给Bob
- Alice选择$k=41$，计算：

$$C_1 = kG = 41\ (2, 2) = (136, 128)$$

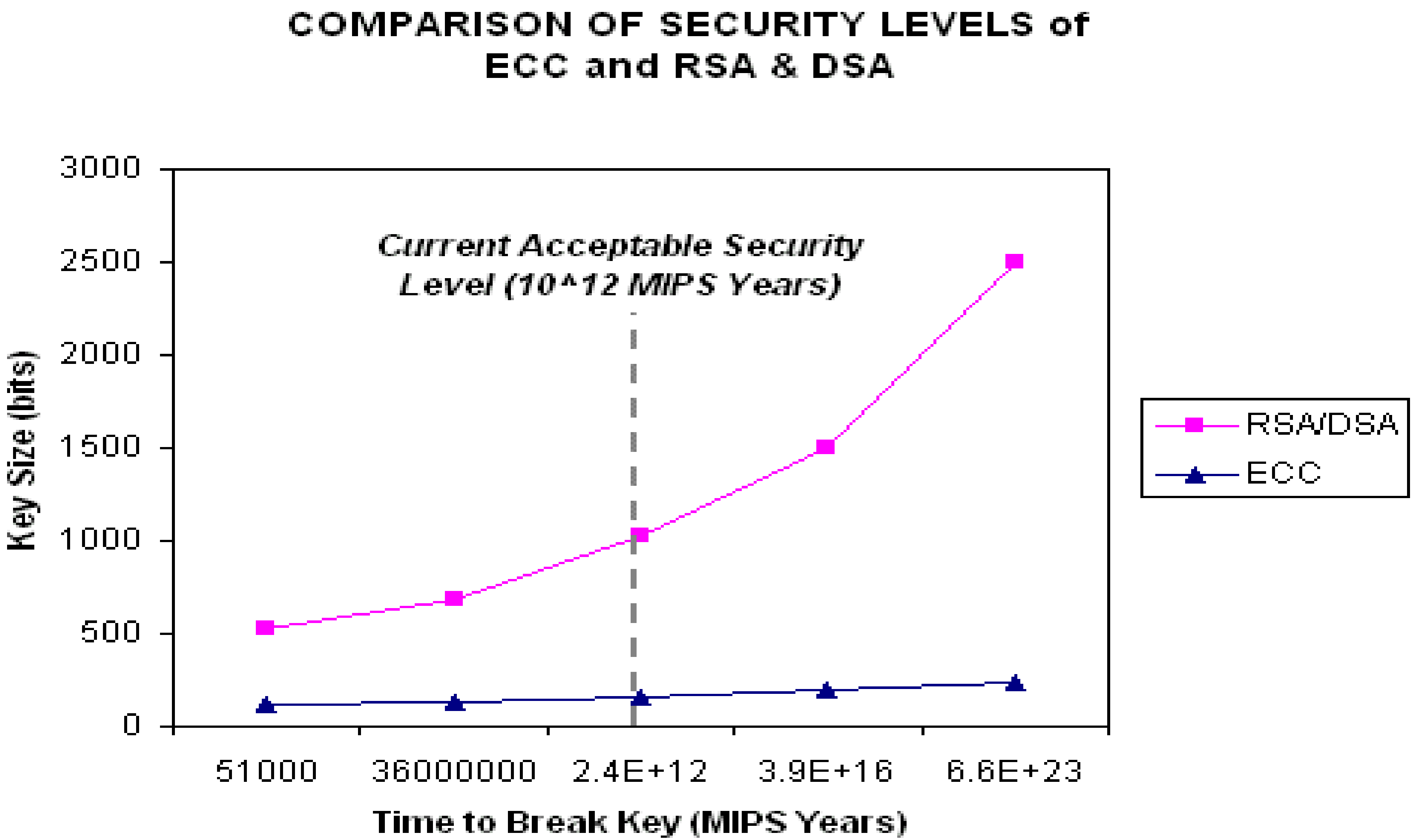
$$kP_B = 41\ (197, 167)=(68, 84)$$

$$C_2=m + kP_B = (112, 26) + (68, 84) = (264, 174)$$

- Alice向Bob发送密文：$C=(C_1, C_2)=\{(136, 128), (246, 174)\}$
- Bob收到密文并计算：$C_2 - n_B C_1 = (264, 174) -101(136, 128)$

$$=(246, 174) - (68, 84) = (112, 26)$$

RSA算法与ECC算法比较



ECC标准 (Drafts & Proposals)

- ANSI X9: 62, 63, 92, …
- IEEE: 1363-2000, P1363a, P1363.2, P802.15.3/4, …
- ISO: 14888-3, 9496, 15496, 18033-2, …
- FIPS: 186-2, 2XX, …
- NESSIE, IPA Cryptrec, …
- SECG: SEC1, SEC2, …
- IETF: PKIX, IPSec, SMIME, TLS, …
- SET, MediaPlayer, 5C, WAP, …

公钥算法功能总结

功能 算法	加密/解密	密钥交换	签名/验证
RSA	是	是	是
ElGamal	是	是	是
ECC	是	是	是
DSA	否	否	是
DH	否	是	否

公钥密码算法总览

- only three types of systems should be considered both **secure** and **efficient**.
- the mathematical problem on which the systems are based:

  - Integer factorization problem (IFP)
  - Discrete logarithm problem (DLP)
  - Elliptic curve discrete logarithm problem (ECDLP)
  - Other mathematical difficult problem

谢谢！