《密码学》

期末速成课

课时五 公钥密码体制

考点	重要程度	占分	题型
1. 常见公钥密码	★★★★	3 - 6	选择/填空
2. RSA	★★★★★	4 - 10	选择/大题
3. ElGamal	★★★	0 - 5	选择/填空
4. ECC	★★★★	2 - 8	选择/大题

一、公钥密码体制

1、常见公钥密码： RSA ECC

2、公钥密码体制核心

单向陷门函数：

单向函数是两个集合X、Y之间的一个映射，使得Y中每个元素y都有唯一的原像x∈X，且由x易于计算它的像y，由y计算它的原像x是不可行的。

$$y = x^3 + \sqrt{x} + x^2 + \frac{2}{x}$$

已知x,求y简单。

已知y,求x简单。

二、RSA

步骤	描述
找出质数	p q
计算	n = p * q
欧拉函数	$\phi(n) = (p-1)(q-1)$
计算公钥 e	$1 < e < \phi(n)$ 且 $\gcd(\phi(n), e)=1$
计算私钥 d	$e * d \% \phi(n) = 1$
加密	$C = M^{E} \bmod N$
解密	$M = C^{D} \bmod N$

二、RSA

公钥{ e , n } 私钥d

【题1】设在RSA公钥密码体制中，公钥(e，n)=(13,35),则私钥d=（ B ）

A.11　　B.13　　C.15　　D.17

解：ed mod φ（n）=1

φ（35）= φ（5） φ（7）= 4×6 = 24

$13d \equiv 1(mod\ 24)$　　1=11-2×5

24=13×1+11　　1=11-（13-11）×5　　-11+24=13

13=11×1+2　　1=11×6-13×5

11=2×5+1　　1=（24-13）×6-13×5

2=1×2+0　　1=24×6-13×11

三、ElGamal

1、密钥产生

密钥产生 → 加密 → 解密

（1）生成随机大素数p，求得p的本原根g

（2）随机选择私钥x，$1<x<p-2$

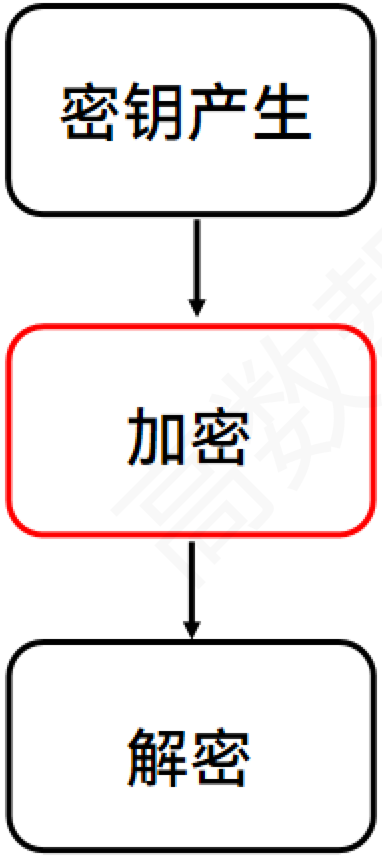
（3）计算$y = g^x \bmod p$

公钥【p，g，y】 私钥【x】

扫码观看
视频讲解更清晰

三、ElGamal

2、加密



（1）从A方获得加密所需的公钥（p,g,y）。

（2）选择一随机数k,（k,p-1）=1,1≤k≤p-2

（3）计算

$$y_1 = g^k \bmod p$$

再用公钥y，计算:

$$y_2 = my^k \bmod p$$

密文c=（y_1, y_2）。

三、ElGamal

3、解密

密钥产生

↓

加密

↓

解密

当A接收到密文$c=(y_1, y_2)$之后解密，使用自己的私钥x计算

$$m = \frac{y_2}{y_1^{x}} \bmod p$$

扫码观看
视频讲解更清晰

四、ECC

椭圆曲线有限域上的加法法则

椭圆曲线E: $y^2 \equiv x^3 + ax + b \pmod{p}$ 椭圆群 $E_p(a, b)$

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

由以下规则确定:

$$x_3 = \lambda^2 - x_1 - x_2 \pmod{p} \qquad y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p}$$

其中

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\[2ex] \dfrac{3x_1^2 + a}{2y_1} & P = Q \end{cases}$$

【题1】以 $E_{23}(1,1)$ 为例，设P=（3，10）,Q=(9,7)，则P+Q=?

解：$\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} \equiv 11 \bmod 23$

$$x_3 = 11^2 - 3 - 9 = 109 \equiv 17 \bmod 23$$

$$y_3 = 11(3-17) - 10 = -164 \equiv 20 \bmod 23$$

所以P+Q=（17，20），仍为 $E_{23}(1,1)$ 中的点。

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & P = Q \end{cases}$$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod{p}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p}$$

【题2】若求2P,则

解：$\lambda=\frac{3\cdot 3^2+1}{2\times 10}=\frac{5}{20}=\frac{1}{4}\equiv 6\bmod 23$

$$x_3=6^2-3-3=30\equiv 7\ mod\ 23$$

$$y_3=6(3-7)-10=-34\equiv 12\ mod\ 23$$

所以2P=（7，12）

$$\lambda=\begin{cases}\frac{y_2-y_1}{x_2-x_1} & P\neq Q\\ \frac{3x_1^2+a}{2y_1} & P=Q\end{cases}$$

$$x_3=\lambda^2-x_1-x_2(\mathrm{mod}p)$$

$$y_3=\lambda(x_1-x_3)-y_1(\mathrm{mod}p)$$

【题3】 已知 $E\left(y^2=x^3-x-2\right)$ 是在有限域 F_{11} 上的椭圆曲线

（1）证明P（1,3），Q（2,2）在该椭圆曲线上;

（2）计算P+Q;　　(3)计算5P.

解:（1） $x^3-x-2=1^3-1-2=-2 \bmod 11=9$

$y^2=3^2=9$ 因此在椭圆曲线上;

$x^3-x-2=2^3-2-2=4$

$y^2=2^2=4$ 因此在椭圆曲线上;

【题3】 已知 $E\left(y^2=x^3-x-2\right)$ 是在有限域 F_{11} 上的椭圆曲线

（1）证明P（1,3），Q（2,2）在该椭圆曲线上;

（2）计算P+Q;　　(3)计算5P.

---

(2)

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1}, P\neq Q\\[2ex]\dfrac{3x_1^2+a}{2y_1}, P=Q\end{cases}$$

$$\lambda=\frac{y_2-y_1}{x_2-x_1}=\frac{2-3}{2-1}=-1 \bmod 11=10$$

$$\begin{cases}x_3=\lambda^2-x_1-x_2=100-1-2=97 \bmod 11=9\\ y_3=\lambda\left(x_1-x_3\right)-y_1=10\left(1-9\right)-3=-83 \bmod 11=5\end{cases}$$

P + Q=（9，5）

【题3】 已知$E\left(y^2=x^3-x-2\right)$是在有限域$F_{11}$上的椭圆曲线

（1）证明P（1,3），Q（2,2）在该椭圆曲线上;

（2）计算P+Q;　　(3)计算5P.

（3） 5P=2P+(2P+P)

$$\lambda_1=\frac{3x_1^2+a}{2y_1}=\frac{3-1}{6}=\frac{1}{3}\bmod 11=4,2P=P+P=(3,0)$$

$$\lambda_2=\frac{y_2-y_1}{x_2-x_1}=\frac{0-3}{3-1}=\frac{-3}{2}\bmod 11=4,2P+P=(1,8)$$

$$\lambda_3=\frac{y_2-y_1}{x_2-x_1}=\frac{8-0}{1-3}=\frac{8}{-2}\bmod 11=7,2P+(2P+P)=(1,3)$$

5P=2P+(2P+P)=(1,3)

【题4】在现有的计算能力条件下，对于非对称密码算法Elgamal，被认为是安全的最小密钥长度是（ D ）。

A.128位　B.160位　C.512位　D.1024位

【题5】在现有的计算能力条件下，对于椭圆曲线密码算法(ECC)，被认为是安全的最小密钥长度是（ B ）。

A.128位　B.160位　C.512位　D.1024位

【题6】第一个实用的、迄今为止应用最广的公钥密码体制是（ A ）。

A. RSA　B.Elgamal　C.ECC　D.NTRU

【题7】公钥密码算法一般是建立在对一个特定的数学难题求解上，那么RSA算法是基于<u>大整数因子分解</u>困难性、ElGamal算法是基于<u>有限域乘法群上离散对数</u>的困难性。

扫码观看
视频讲解更清晰