第十章作业

16337341 朱志儒

思考题

10.1 Diffie-Hellman 密钥交换：素数 q 和其本原根 a 是两个公开的整数。假定用户 A 和 B 希望交换密钥，那么用户 A 选择一个随机整数$X_A < q$，并计算$Y_A = a^{X_A} \ mod \ q$，用户 B 也独立地选择一个随机整数$X_B < q$，并计算$Y_B = a^{X_B} \ mod \ q$，A 和 B 保持其 X 是私有的，Y 是公开可访问的，用户 A 计算$K = (Y_B)^{X_A} \ mod \ q$并将其作为密钥，用户 B 计算$K = (Y_A)^{X_B} \ mod \ q$并将其作为密钥。

10.2 椭圆曲线: 椭圆曲线与计算椭圆周长的方程相似, 一般, 椭圆曲线的三次方程形为$y^2 + axy + by = x^3 + cx^2 + dx + e$，其中 a，b，c，d，e 是实数，x 和 y 在实数集上取值。

10.3 椭圆曲线的零点是加法的单位元。

10.4 椭圆曲线上同在一条直线上的三个点的和为 O。

习题

10.1 （a）$Y_A = 7^5 \bmod 71 = 51$

（b）$Y_B = 7^{12} \bmod 71 = 4$

（c）$K = 4^5 \bmod 71 = 30$

10.2 （a）$\varphi(11) = 10$

$2^{10} = 1024 = 1 \bmod 11$
$2^n \neq 1 \ mod \ 11 \ (n < 10)$

（b）$X_A = 6$，因为$2^6 \ mod \ 11 = 9$。

（c）$K = 3^6 \bmod 11 = 3$

10.4 $X_A = 5, X_B = 3, K = (3^3)^5 = 14348907$

10.6 （a）密文：$(49, 57)$

（b）$C_2 = 29$

10.7 （a）$2Q = O$

（b）$3Q = 2Q + Q = O + Q = Q$

10.9 方程左边 $= 7^2 = 49$

方程右边 $= 4^3 - 5 \times 4 + 5 = 49$

所以点（4，7）在椭圆曲线上。

10.10 计算 $R = P + Q$：

$$\Delta = (8.5 - 9.5)/(-2.5 + 3.5) = -1$$

$$x_R = 1 + 3.5 + 2.5 = 7$$

$$y_R = -8.5 - (-3.5 - 7) = 2$$

$$R = (7, 2)$$

计算 2P：

$$x_r = [(36.75 - 36)/19]^2 + 7 \approx 7$$

$$y_R = [(36.75 - 36)/19](-3.5 - 7) - 9.5 \approx 9.9$$

10.12

x	$(x^3 + x + 6) \bmod 11$	模 p 的平方根?	y
0	6	no	
1	8	no	
2	5	yes	4, 7

3	3	yes	5, 6
4	8	no	
5	4	yes	2, 9
6	8	no	
7	4	yes	2, 9
8	9	yes	3, 8
9	7	no	
10	4	yes	2, 9

10.14

2G = (5, 2)	3G = (8, 3)	4G = (10, 2)	5G = (3, 6)
6G = (7, 9)	7G = (7, 2)	8G = (3, 5)	9G = (10, 9)
10G = (8, 8)	11G = (5, 9)	12G = (2, 4)	13G = (2, 7)

10.16 （a）$P_B = n_B$ x G = 7 x (2, 7) = (7, 2)

（b）$C_m = \{kG, P_m + kP_B\} = \{3(2, 7), (10, 9) + 3(7, 2)\} = \{(8,3), (10, 9) + (3, 5)\} = \{(8, 3), (10, 2)\}$

（c）$P_m = (10, 2) - 7(8, 3) = (10, 2) - (3, 5) = (10, 2) + (3, 6) = (10, 9)$