

CSCI 381 - Advanced Cryptography - Fall 2005
George Washington University

Homework II

due 5 October

10%

Show all work. You will be graded almost entirely on how you get to the solution, and not on whether you get there. More efficient and elegant solutions will receive higher marks.

1. Consider the elliptic curve $y^2 = x^3 + 1$ over the reals. Compute the value of $5P$ for $P = (2, 3)$ using efficient exponentiation showing all steps.
2. Let P be a point on an elliptic curve over the reals. Suppose that P is not the point at ∞ . Give a geometric condition that is equivalent to P being a point of order (a)2; (b)3; (c)4.
3. Determine the number of points on the elliptic curve $y^2 = x^3 + x + 1$ over \mathbb{Z}_7^* . Is the group of points on that curve cyclic? If so, determine a generator of the group.
4. Let p be a prime number $p \equiv 3 \pmod{4}$ and let E be the elliptic curve $y^2 = x^3 + ax + b \pmod{p}$. Find a polynomial time algorithm that, given $x \in \mathbb{Z}_p^*$, computes a point (x, y) on E if it exists. Hint: show that, if a is a square \pmod{p} , $a^{\frac{p+1}{4}}$ is a square root of $a \pmod{p}$. Using this algorithm, find the point $(2, y)$ on the curve $y^2 = x^3 + x^2 + 1 \pmod{111119}$.
5. It is trivial that public-key encryption cannot be perfectly secret. If $\langle K, \hat{K} \rangle$ is a public-private key pair, where K is the public key, and assuming the system is not trivial, show (in a few lines each) that:
 - A. $p(m|E_K(m)) \neq p(m)$ and
 - B. $p(\hat{K}|K) \neq p(\hat{K})$. Hint: if K is known, so is $E_K(m)$ for any m .

You may not assume that, given a public key, a private key is uniquely defined.

Notice that information leakage regarding the private key does not require message encryption by the private key, the public key itself leaks the information.