T-79.503 Foundations of Cryptology
Homework 12
December 10, 2003

1. Let E be the elliptic curve $y^2 = x^3 + x + 13$ defined over $\mathbb{Z}_{31}$ (see Homework 11).

   a) Show that $34(9, 10) = \mathcal{O}$.

   b) Show that (9,10) is an element of order 34 with respect to the elliptic curve group operation.

2. (Stinson 6.18)

   a) Determine the NAF representation of the integer 87.

   b) Using the NAF representation of 87, use Algorithm 6.5 to compute $87P$, where $P = (2, 6)$ is a point on the elliptic curve $y^2 = x^3 + x + 26$ defined over $\mathbb{Z}_{127}$. Show the partial results during each iteration of the algorithm.

3. Consider $p = 2003$, which is a prime. Find an element of order $q = 11$ in the multiplicative group $\mathbb{Z}^*_{2003}$.

4. Consider a variation of El Gamal Signature Scheme in $GF(2^n)$. The public parameters are n, q and α, where q is a divisor of $2^n - 1$ and α is an element of $GF(2^n)$ of multiplicative order q. A user's secret key is $a \in \mathbb{Z}_q$ and the public key β is computed as $\beta = \alpha^a$. To generate a signature for message x a user with secret key a generates a secret value $k \in \mathbb{Z}^*_q$ and computes the signature (γ, δ) as

$$\begin{aligned} \gamma &= \alpha^k \text{ (in } GF(2^n)) \\ \delta &= (x - a\gamma')k^{-1} \bmod q, \end{aligned}$$

   where γ' is an integer representation of γ. Suppose Bob is using this signature scheme, and he signs two messages x_1 and x_2, and gets signatures (γ_1, δ_1) and (γ_2, δ_2), respectively. Alice sees the messages and their respective signatures, and she observes that $\gamma_1 = \gamma_2$.

   a) Describe how Alice can now derive information about Bob's private key.

   b) Suppose $n = 8$, $q = 15$, $x_1 = 1$, $x_2 = 4$, $\delta_1 = 11$, $\delta_2 = 2$, and $\gamma'_1 = \gamma'_2 = 7$. What Alice can say about Bob's private key?

5. Consider a variation of the ElGamal Signature Scheme giving message recovery. The public parameters of this scheme are odd primes p and q such that q divides $p - 1$, and an element α of the field $\mathbb{Z}_p$ such that the multiplicative order of α is equal to q. A user's private key is an integer a such that $1 < a < q$, and the user's public key β is computed as $\beta = \alpha^a \bmod p$. A signature of a message $x \in \mathbb{Z}_q$ is a pair (γ, δ), where $\gamma \in \mathbb{Z}_q$ and $\delta \in \mathbb{Z}_q$ are produced as follows: The user generates a secret random integer k such that $1 < k < q$ and computes

$$\begin{aligned} \gamma &= (x - (\alpha^k \bmod p)) \bmod q \\ \delta &= (k - a\gamma) \bmod q. \end{aligned}$$

a) Show how the message x can be recovered from the signature (γ, δ) given the public parameters p, q, α and β.

b) Let $p = 1999$ and $q = 37$. Show that the multiplicative order of the element $\alpha = 2^{54} \bmod 1999 = 1278$ is equal to 37.

c) Using parameters p, q and α given above in b), generate a secret and a public key for yourself.

d) Generate your signature for a message $x \in \mathbb{Z}_{37}$ of your choice.