T-79.5501 Cryptology
Homework 11
December 7 & 8, 2005

1. (Stinson 6.18) In elliptic curves computing $-P$ given a point P is trivial, compared to finite multiplicative groups based on fields where the analogical operation is taking inverses (using the Euclidean algorithm). By this property the double-and-add algorithm for point multiplication can be speeded up by using a NAF representation of the multiplier (see Section 6.5.5).
   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.

2. Consider $p = 1231$, which is a prime. Find an element of order $q = 41$ in the multiplicative group $\mathbb{Z}^*_{1231}$.

3. 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) Given parameters p, q and α as in b), assume the private key is $a = 8$. Compute the public key.
   d) Compute a signature of the message $x = 12$ using the private key and show how the signature is verified.

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 $\beta = \alpha^a$ in $GF(2^n)$. 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?