T-79.5501 Cryptology Spring 2009

Homework 11

Tutor : Joo Y. Cho
joo.cho@tkk.fi

30th April 2009

Q1. Let E be the elliptic curve $y^2 = x^3 + 2x + 7$ defined over $\mathbb{F}_{31}$ (see Homework 11). Compute the decompressions of $(18, 1)$, $(3, 1)$, $(17, 0)$ and $(28, 0)$.

A1.
The curve E is given

$$E(\mathbb{F}_{31}) : y^2 = x^3 + 2x + 7. \quad (1)$$

For this problem we can just look them up from the previous computations. For example, DECOMPRESS(3,1) is

$$y^2 = 3^3 + 2 \cdot 3 + 7 = 40 \equiv 9 = 3^2 \bmod 31$$

Since $y = 3 \equiv 1 \bmod 2$, we get (3,1). So $b = y \mod 2$ identifies which y to use—the odd one or the even one.

$$P_1 = \textsc{decompress}(18, 1) = (18, 27)$$
$$P_2 = \textsc{decompress}(3, 1) = (3, 3)$$
$$P_3 = \textsc{decompress}(17, 0) = (17, 26)$$
$$P_4 = \textsc{decompress}(28, 0) = (28, 6).$$

Q2. Let E be as above. As shown in Homework 11, $\#E = 39$ and $P = (2, 9)$ is an element of order 39 in E. The *Simplified ECIES* defined on E has $\mathbb{F}_{31}^*$ as its plaintext space. Suppose the private key is $a = 8$.

a) Compute $Q = aP$.

b) Decrypt the following string of ciphertext:

$$((18, 1), 21), ((3, 1), 18), ((17, 0), 19), ((28, 0), 8)$$

A2.

1. We compute $8P = 2^3P = 2(2(2P))$ using three doublings.

$$\begin{aligned} 2P &= (10, 2) \\ 4P &= 2(2P) = (15, 8) \\ 8P &= 2(4P) = (8, 15). \end{aligned}$$

2. We proceed as in the textbook using the decompressions P_i from above, computing mP_i:

$$\begin{aligned} 8P_1 &= (15, 8) \\ 8P_2 &= (2, 9) \\ 8P_3 &= (30, 29) \\ 8P_4 &= (14, 19). \end{aligned}$$

We use these *x*-coordinates to recover the plaintext:

$$21 \cdot (15)^{-1} \mod 31 = 21 \cdot 29 \mod 31 = 20 = \text{'T'}$$
$$18 \cdot (2)^{-1} \mod 31 = 18 \cdot 16 \mod 31 = 9 = \text{'I'}$$
$$19 \cdot (30)^{-1} \mod 31 = 19 \cdot 30 \mod 31 = 12 = \text{'L'}$$
$$8 \cdot (14)^{-1} \mod 31 = 8 \cdot 20 \mod 31 = 5 = \text{'E'}$$

and the plaintext is “TILE”.

Q3.

Let p be prime and $p > 3$. Show that the following elliptic curves over $\mathbf{Z}_p$ have $p+1$ points:

a) $y^2 = x^3 - x$, for $p \equiv 3 (\mathrm{mod} 4)$. Hint: Show that from the two values $\pm r$ for $r \neq 0$ exactly one gives a quadratic residue modulo p.

b) $y^2 = x^3 - 1$, for $p \equiv 2 (\mathrm{mod} 3)$. Hint: If $p \equiv 2 (\mathrm{mod} 3)$, then the mapping $x \mapsto x^3$ is a bijection in $\mathbf{Z}_p$.

A3-a). Let the map $\mathcal{X} : \mathbb{F}_p^\times \to C_2$ be defined by $\mathcal{X}(u) \mapsto \left(\frac{u}{p}\right)$ (the Legendre symbol). So $\mathcal{X}(u)$ maps u to 1 if it has a square root, -1 if it does not, or 0 if it is zero. It clearly follows

$$\#\{y \in \mathbb{F}_p : y^2 = u\} = 1 + \mathcal{X}(u)$$

From the Legendre symbol rules when $p \equiv 3 \pmod 4$ we have

$$\mathcal{X}((-x)^3 - (-x)) = \mathcal{X}(-1)\mathcal{X}(x^3 - x) = -\mathcal{X}(x^3 - x)$$

Hence, $\sum_{x \in \mathbb{F}_p} \mathcal{X}(x^3 - x) = 0$ and we have

$$\#E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} (1 + \mathcal{X}(x^3 - x)) = 1 + p + \sum_{x \in \mathbb{F}_p} \mathcal{X}(x^3 - x) = 1 + p.$$

A3-b).

- We can consider more generally $y^2 = x^3 + b$ over $\mathbb{F}_p$ with $p \equiv 2 \pmod 3$.
- The problem hints $x \mapsto x^3$ is a bijection, thus cubed roots are unique.
- Given a y-coordinate, we solve for x using $x = \sqrt[3]{y^2 - b}$ which has exactly one solution—that is, for every $y \in \mathbb{F}_p$ we get exactly one point $(\sqrt[3]{y^2 - b}, y) \in E(\mathbb{F}_p)$.
- This gives us $\#\mathbb{F}_p = p$ points, and including the identity $\mathcal{O}$ we find $\#E(\mathbb{F}_p) = p + 1$.
- In general, the following form of *supersingular* elliptic curves have $p + 1$ points: $E : y^2 = x^3 - ax$ over $\mathbb{F}_p$ where $p \equiv 3 \pmod 4$ and $E : y^2 = x^3 + b$ over $\mathbb{F}_p$ where $p \equiv 2 \pmod 4$.

Q4.

Let $E = E(\mathbb{F}_{43})$ be the elliptic curve $y^2 = x^3 + 32x$ presented in Lecture 11. The purpose of this problem is to show that E is isomorphic to $\mathbf{Z}_{22} \times \mathbf{Z}_2$. It is possible to do it without computing a single elliptic curve point operation.

Denote $P = (41, 10) \in H_2$ and $Q = (0, 0) \in H_1$. Then ord(P)= 22 and ord(Q)= 2.

1. Prove that ord($P + Q$)= ord($2P + Q$)= 22 and $P + Q \in H_3$ and $2P + Q \in H_1$.
2. Let us consider the cyclic subgroups $H_1 = \langle 2P + Q \rangle$, $H_2 = \langle P \rangle$ and $H_3 = \langle P + Q \rangle$. Show that, for any $S \in E$, $S \in H_1 \cap H_2 \cap H_3$ if and only if $S = mP$, where m is even.
3. Show that all points $S \in E$ admit a unique representation in the form $aP + bQ$, where $a \in \mathbf{Z}_{22}$ and $b \in \mathbf{Z}_2$.
4. Show that the mapping $\phi : E \to \mathbf{Z}_{22} \times \mathbf{Z}_2$, $\phi(aP + bQ) = (a, b)$ is an isomoprphism.

A4-a). Given $P \in H_2$, $Q \in H_1$, $\langle P \rangle = H_2$ and $\langle Q \rangle = \{(0,0), \mathcal{O}\}$, we observe $\langle P \rangle \cap \langle Q \rangle = \mathcal{O}$. It follows that

if $aP = bQ$ for some integers a and b, then $a \equiv 0 \bmod 22$ and $b \equiv 0 \bmod 2$. (*)

- Claim 1: $\mathrm{ord}(P+Q) = 22$.

$$2(P+Q) = 2P \neq \mathcal{O} \Rightarrow \mathrm{ord}(P+Q) \neq 2$$
$$11(P+Q) = 11P + 11Q \neq \mathcal{O} \text{ by (*) } \Rightarrow \mathrm{ord}(P+Q) \neq 11,$$

- Claim 2: $\mathrm{ord}(2P+Q) = 22$.

$$2(2P+Q) = 4P \neq \mathcal{O} \Rightarrow \mathrm{ord}(2P+Q) \neq 2$$
$$11(2P+Q) = 11Q \neq \mathcal{O} \Rightarrow \mathrm{ord}(2P+Q) \neq 11.$$

A4-a).

- Claim 3: $(P+Q) \in H_3$

  If $P+Q \in H_1$, then $P \in H_1$ since $Q \in H_1$, which is contradiction. Hence, $P+Q \neq H_1$. Similarly, $P+Q \neq H_2$. Since $E = H_1 \cup H_2 \cup H_3$, we conclude $P+Q \in H_3$.

- Claim 4: $(2P+Q) \in H_1$

  Since $2P \in H_1$ and $Q \in H_1$, the claim follows.

A4-b) and c).

- If $\langle 2P \rangle \subset H_1 \cap H_2 \cap H_3$, then $mP \in H_1 \cap H_2 \cap H_3$ for even m. To prove the contrary, let $S \in H_1 \cap H_2 \cap H_3$. Then, we have

$$S \in H_2 = \langle P \rangle \Rightarrow S = aP, a \in \mathbf{Z}_{22}$$
$$S \in H_3 = \langle P + Q \rangle \Rightarrow S = b(P+Q), b \in \mathbf{Z}_{22}.$$

  By (*), $bP + bQ = aP \Rightarrow (a-b)P = bQ$. Hence, $a = b \bmod 22$ and $b = 0 \bmod 2$. It follows that $a = 0 \bmod 2$.

- Assume that $S \in E$ is represented by $a_1P + b_1Q$ and $a_2P + b_2Q$ where $a_1 \neq a_2$ or $b_1 \neq b_2$. Then,

$$a_1P + b_1Q = a_2P + b_2Q \Rightarrow (a_1 - a_2)P = (b_2 - b_1)Q$$

  From (*), we have $a_1 = a_2 \bmod 22$ and $b_1 = b_2 \bmod 2$ so the claim follows.

A4-d).

- From (a), $S \in E$, S can be represented in a form $aP + bQ$.
- From (c), $S = aP + bQ$ is a unique representation.
- Hence, $\phi : E \longrightarrow \mathbf{Z}_{22} \times \mathbf{Z}_2, S \mapsto aP + bQ$ is one-to-one.
- Since $\#E = 44 = \#\{\mathbf{Z}_{22} \times \mathbf{Z}_2\}$, ϕ is bijective.
- Clearly ϕ represents the group operation $\phi(S_1 + S_2) = (a_1 + a_2, b_1 + b_2)$ for all $S_1 = a_1P + b_1Q \in E$ and $S_2 = a_2P + b_2Q \in E$.

Q5. Let E be as in Problem 1 and 2.

a) Determine the NAF representation of the integer 27.

b) Using the NAF representation of 27, use Algorithm 6.5 to compute $27P$, where $P = (2, 9)$.

A5. NAF stands for Non-Adjacent Form—no two coefficients are non-zero. If q_i is odd, then $k_i = 2 - (q_i \mod 4)$. else $k_i = 0$. Also, $q_{i+1} = (q_i - k_i)/2$.

i	q_i	$q_i \mod 4$	k_i
0	27	3	-1
1	14	—	0
2	7	3	-1
3	4	—	0
4	2	—	0
5	1	1	1

so $27 = 2^5 - 2^2 - 1$ and we have NAF(27)=(1,0,0,-1,0,-1) of weight 3 and length 6.

Given the NAF above and $P = (2, 9)$, we calculate $27P$ as

$$2(2(2(2(2P)) - P)) - P$$

outlined below. To subtract P we add $-P = (x, -y)$.

i	k_i	Double	Sub	Result
4	0	2(2,9) = (10,2)	—	
3	0	2(10,2) = (15,8)	—	
2	-1	2(15,8) = (8,15)	-(2,9)	(6,24)
1	0	2(6,24) = (20,24)	—	
0	-1	2(20,24) = (30,2)	-(2,9)	(9,14)

and $27 \cdot (2, 9) = (9, 14)$.

Q6.

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 $a \in \mathbf{Z}_q$ 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 $k \in \mathbf{Z}_q^*$ 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?

A6-a.

With $k_i \in_R \mathbf{Z}_q^*$, observing $\gamma_1 = \gamma_2 \Rightarrow k_1 = k_2$ as $\text{ord}(\alpha) = q$; the same nonce has been used twice. We will denote $k_1 = k_2 = k$ and $\gamma_1 = \gamma_2 = \gamma$.

1. From the construction of the δ_i signature portions, we get the following system of equations:

$$k = (x_1 - a\gamma')\delta_1^{-1} \mod q$$
$$k = (x_2 - a\gamma')\delta_2^{-1} \mod q.$$

   We have two equations and two unknowns (k, a) and simply solve algebraically for the private key a by eliminating k. We find

$$a = (x_2\delta_1 - x_1\delta_2)(\gamma'\delta_1 - \gamma'\delta_2)^{-1} \mod q.$$

A6-b.

- We use the above equation and find

$$a = (4 \cdot 11 - 1 \cdot 2)(7 \cdot 11 - 7 \cdot 2)^{-1} = 12 \cdot (3)^{-1} \mod 15$$

- but 3 is not relatively prime to 15 and has no inverse.
- We do however find

$$3a = 12 \mod 15 \Rightarrow 3a = 12+15i \Rightarrow a = 4+5i \Rightarrow a \equiv 4 \pmod 5$$

and thus $a \in \{4, 9, 14\}$. Given a public key we could easily test these three values.