Cryptography and Security 2017

Solution Sheet 6

Solution 1 Computation in GF(2^k) and Linear Algebra

1. (a) $X^3 + X + 1$ is irreducible because it has no roots (only correct for polynomials of degree 2 and 3), while $X^3 + 1$ is reducible.

   (b) $X^3 + X + 1$ is irreducible so it can not be factored, but we can factor $X^3 + 1$ as $X^3 + 1 = (X + 1)(X^2 + X + 1)$.

   (c) $2^3 = 8$ elements.

   (d) $x^2 = x \rightarrow x^2 + x = 0 \rightarrow x(x + 1) = 0$, so $x = 0, x = 1$ are solutions, but as we are in a field and the degree of the polynomial is 2 we can not have more roots.

   (e) $< X >= \{1, X, X^2, X + 1, X^2 + X, X^2 + X + 1, X^2 + 1\}$

   (f) $x^2 = 1 \rightarrow (x + 1)(x - 1) = 0$, so we have only one solution $x = 1$ over GF(2)(2), but to prove that we have no more solutions, we say that all of the roots of this equation form a subgroup of $F\backslash\{0\}, \times$ (we can simply show it!), so the order of this subgroup should divide the order of the group, while the order of the group is 7, so we can have only one solution. In GF(3), we have two solutions $x = 1$ and $x = 2$.

   (g) In $\mathbb{Z}_n$ with $n = pq$ as a product of two large primes, we need to solve $x^2 \equiv 1 \bmod pq$, while by CRT we can rewrite it as $x^2 \equiv 1 \bmod p$ and $x^2 \equiv 1 \bmod q$, so we will have

   $$\begin{cases} x \equiv 1 \bmod p \\ x \equiv -1 \bmod p \end{cases} \qquad \begin{cases} x \equiv 1 \bmod q \\ x \equiv -1 \bmod q \end{cases}$$

   So, for the system of equations to pick and solve by CRT we have 4 options, so we will get 4 solutions using CRT. If we work in $\mathbb{Z}_6$, then the first two equations in the system above would be equal and so we will get only 2 solutions using CRT. We can not use CRT in $\mathbb{Z}_4$, because 2 and 2 are not coprime, so the only way is to exhaustively search for all possible solutions and we will obtain 2 solutions.

   (h) We have $Sq(X + Y) = (X + Y)^2 = X^2 + Y^2 + 2XY = X^2 + Y^2 = Sq(X) + Sq(Y)$. To show that Sq is one-one, first we claim that $Sq(X) = 0$ leads to $X = 0$, that is because $F\backslash\{0\}$ is a cyclic multiplicative group that there is no element in $F\backslash\{0\}$ with $X^2 = 0$, so $Sq(X) = 0$ leads to $X = 0$. Then we can check that $Sq(X - Y) = Sq(X) + Sq(Y)$. To prove that it is injective we need to show that if $Sq(Y) = Sq(X)$ leads to $X = Y$. We have $Sq(X) - Sq(Y) = Sq(X - Y) = 0$. Therefore, $X = Y$, so the function is injective. As Sq is from F to F, so it is surjective as well, so it is bijective.

2. Let us consider the polynomial $P(X) = X^4 + X + 1$ in $\mathbf{Z}_2[X]$.

   (a) $P(0) = 1$ and $P(1) = 1$, so it has no roots.

   (b) Having no root is equivalent to having no factor of degree 1 in $\mathbf{Z}_2[x]$.

   (c) $\{X^2, X^2 + 1, X^2 + X, X^2 + X + 1\}$ and $X^2 + X + 1$ is irreducible.

   (d) If you divide $P(X)$ by $Q(X)$, you will see the remainder is not zero.

   (e) $P(X)$ has no roots and is not divisible by the only irreducible polynomial of degree two so it is irreducible.

Solution 2 Elliptic Curves and Finite Fields I

1. The multiplication table of the elements of $\mathbf{K}$ is given in Table 1.

Table 1: Multiplication table of $\mathbf{Z}_7$

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

2. Let $P = (x, y)$ be a point of $\mathrm{E}_{2,1}$.

   - If $x = 0$, y must satisfy $y^2 = 1$, so that $(0, 1)$ and $(0, 6)$ are points of $\mathrm{E}_{2,1}$.
   - If $x = 1$, y must satisfy $y^2 = 4$, so that $(1, 2)$ and $(1, 5)$ are points of $\mathrm{E}_{2,1}$.
   - If $x = 2$, y must satisfy $y^2 = 6$, which is impossible.
   - If $x = 3$, y must satisfy $y^2 = 6$, which is impossible.
   - If $x = 4$, y must satisfy $y^2 = 3$, which is impossible.
   - If $x = 5$, y must satisfy $y^2 = 3$, which is impossible.
   - If $x = 6$, y must satisfy $y^2 = 5$, which is impossible.

   Finally $\mathrm{E}_{2,1} = \{\mathcal{O}, (0, 1), (0, 6), (1, 2), (1, 5)\}$ and thus $|\mathrm{E}_{2,1}| = 5$. According to Hasse's Theorem, we should have $||\mathbf{K}| + 1 - |\mathrm{E}_{2,1}|| \leq 2\sqrt{|\mathbf{K}|}$. As $||\mathbf{K}| + 1 - |\mathrm{E}_{2,1}|| = 7 + 1 - 5 = 3$ and $2\sqrt{|\mathbf{K}|} = 2\sqrt{7} > 3$, everything is fine.

3. Table 2 confirms that $-P$ lies on the curve as well.

Table 2: Inverse elements of $\mathrm{E}_{2,1}$

P	$\mathcal{O}$	$(0, 1)$	$(0, 6)$	$(1, 2)$	$(1, 5)$
$-P$	$\mathcal{O}$	$(0, 6)$	$(0, 1)$	$(1, 5)$	$(1, 2)$

4. As $\mathrm{E}_{2,1}$ is a group of prime order, each of its elements (except $\mathcal{O}$) is a generator. This is because the order of an element should divide $|\mathrm{E}_{2,1}|$, which is prime, so that the order of an element is either 1 (this is only the case for $\mathcal{O}$) or $|\mathrm{E}_{2,1}|$. We choose for example $G = (1, 2)$ as a generator. Consider the mapping

$$\begin{array}{rccc} \varphi: & \mathbf{Z}_5 & \longrightarrow & \mathrm{E}_{2,1} \\ & \gamma & \longmapsto & \gamma G. \end{array}$$

   It is easy to show that φ is a group isomorphism. From

$$\begin{array}{rcll} \varphi(\alpha + \beta) & = & (\alpha + \beta)G & \\ & = & \alpha G + \beta G & \text{(by associativity of + in } \mathrm{E}_{2,1}) \\ & = & \varphi(\alpha) + \varphi(\beta), & \end{array}$$

   φ is a group homomorphism. As

$$\begin{array}{rcll} \varphi(\gamma) = 0 & \Rightarrow & \gamma G = \mathcal{O} & \\ & \Rightarrow & \gamma = 0 & \text{(as } G \text{ is a generator of } \mathrm{E}_{2,1}), \end{array}$$

Table 3: Elements generated by a generator G in $\mathrm{E}_{2,1}$

G	$2G$	$3G$	$4G$	$5G$
$(1,2)$	$(0,1)$	$(0,6)$	$(1,5)$	$\mathcal{O}$

φ is injective. As $|\mathbf{Z}_5| = |\mathrm{E}_{2,1}|$, φ is an isomorphism. Therefore, $\mathrm{E}_{2,1}$ is isomorphic to $\mathbf{Z}_5$. Note that an isomorphism is *very* useful to compute the addition table of the points of the elliptic curve. Indeed, after some computations, one can obtain Table 3.

From the definition of the isomorphism φ, we have the following correspondence between the elements of $\mathrm{E}_{2,1}$ and of $\mathbf{Z}_5$:

$$\begin{aligned} \mathcal{O} &\leftrightarrow 0 \\ (1,2) &\leftrightarrow 1 \\ (0,1) &\leftrightarrow 2 \\ (0,6) &\leftrightarrow 3 \\ (1,5) &\leftrightarrow 4 \end{aligned}$$

The addition table of the elements of $\mathbf{Z}_5$ is given in Table 4.

Table 4: Addition table of $\mathbf{Z}_5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

From this, we easily obtain the addition table of the elements of $\mathrm{E}_{2,1}$ which is given in Table 5.

Table 5: Addition table of $\mathrm{E}_{2,1}$

$+$	$\mathcal{O}$	$(1,2)$	$(0,1)$	$(0,6)$	$(1,5)$
$\mathcal{O}$	$\mathcal{O}$	$(1,2)$	$(0,1)$	$(0,6)$	$(1,5)$
$(1,2)$	$(1,2)$	$(0,1)$	$(0,6)$	$(1,5)$	$\mathcal{O}$
$(0,1)$	$(0,1)$	$(0,6)$	$(1,5)$	$\mathcal{O}$	$(1,2)$
$(0,6)$	$(0,6)$	$(1,5)$	$\mathcal{O}$	$(1,2)$	$(0,1)$
$(1,5)$	$(1,5)$	$\mathcal{O}$	$(1,2)$	$(0,1)$	$(0,6)$

Solution 3 Encoding Messages in Elliptic Curves

1. We have $rQ = rdP = dR$. This is actually the Diffie-Hellman property: the receiver selects a long-term secret d and a public key $Q = dP$ and the sender selects an ephemeral secret r and a public $R = rP$. The key on which they agree is rdP, computed as rQ on the sender side and as dR on the receiver side.

   The cryptosystem is performing this Diffie-Hellman-like protocol, then encrypt the point M by the generalized Vernam cipher with key rdP, i.e., by adding these two points.

   So, $M = S - dR$ which is computed with the secret d and the ephemeral public key R from the ciphertext. Thus, $m = \mathsf{map}^{-1}(S - dR)$.

2. We need map to

- map bitstrings to the group spanned by P (i.e., the entire elliptic curve, since P generates it by assumption),
- to be easy to compute,
- to be injective (to be invertible),
- and to have its inverse easy to compute.

First of all, the output of map is clearly in the group spanned by P.

To make it invertible, we must restrict the length of m to $\log_2 n$.

Then, we realize that computing map^{-1} is hard since it consists of computing a discrete logarithm in the elliptic curve. So, this function is not usable.

3. If the computation works, $\mathsf{map}(m)$ is clearly a point of the elliptic curve.

   To make it invertible, we must restrict the length of m to $\log_2 p$. Then, $\mathsf{map}^{-1}(x, y) = \mathsf{integer}^{-1}(x)$. So, we only have to convert an integer into a bitstring, which is easy to do.

   One problem is that $y^2 = x^3 + ax + b$ has a solution if and only if $x^3 + ax + b$ is a quadratic residue, and this is not guaranteed. So, m may have no image by map.

4. To evaluate map, we increment i from 0 until $\left(\frac{x^3+ax+b}{p}\right) = +1$, for $x = 2^k\mathsf{integer}(m) + i$. Then, we take y the smallest integer such that $y^2 = x^3 + ax + b$ and set $\mathsf{map}(m) = (x, y)$.

   We define $\mathsf{map}^{-1}(x, y) = \mathsf{integer}^{-1}\left(\lfloor \frac{x}{2^k} \rfloor\right)$.

   This function seems to satisfy our needs, but the distribution of $\mathsf{map}(m)$ is not so good (some points have no preimage), the complexity is not so nice (we may need to test quadratic residuosity for several values), and we may be careful that $\mathsf{map}(\mathsf{map}^{-1}(x, y))$ may not be equal to (x, y).

5. A random value in $\mathbf{Z}_p$ has a square root with probability roughly $\frac{1}{2}$. By rough estimates, a set of 2^k random values has all its elements with no square root with probability 2^{-2^k}.

   We can encrypt up to $p2^{-k}$ possible plaintexts. Let S be the size of the plaintext space, between 2 and $p2^{-k}$. We have S sets of 2^k random values. Finally, the probability that one of the S set is like this is between 2^{-2^k} and $S2^{-2^k}$, depending on S.

   In the worst case, we have $S = p2^{-k}$. We can just take $k = 9$ and have a probability lower than 2^{-80} in any case.