Cryptography and Security 2017

Exercise Sheet 6

Exercise 1 Computation in $\mathsf{GF}(2^k)$ and Linear Algebra

1. Let $\mathsf{GF}(2)$ be a field with two elements.

   (a) Look at these two polynomials X^3+1 and X^3+X+1. Which one is irreducible in $\mathsf{GF}(2)[X]$? Let $P(X)$ be this polynomial and $Q(X)$ be the other. Give a complete proof that $P(X)$ is indeed irreducible.

   (b) Factor $P(X)$ and $Q(X)$ in $\mathsf{GF}(2)[X]$.

   (c) We define a field F as the set of all polynomials modulo $P(X)$, or in other terms $F = \mathsf{GF}(2)[X]/P(X)$, with the addition and multiplication of polynomials modulo $P(X)$. How many elements does this field have?

   (d) How many solutions in F does the equation $x^2 = x$ have? Write all of them and prove that there is no more?

   (e) Compute $1, X, X^2, \ldots$ modulo $P(X)$.

   (f) How many solutions in $\mathsf{GF}(2)$ does the equation $x^2 = 1$ have? How many solutions in F? Prove that there is no more. How about $\mathsf{GF}(3)$?

   (g) How about in $\mathbf{Z}_n$ with $n = pq$ as a product of two large primes? How about in $\mathbf{Z}_6$ and $\mathbf{Z}_4$?

   (h) Let $Sq : F \to F$ be defined as $Sq(x) = x^2$ in $\mathsf{GF}(2)[X]/P(X)$. Show that $Sq(x+y) = Sq(x) + Sq(y)$? Show that Sq is one-to-one (bijective)?

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

   (a) Show that P has no root in $\mathbf{Z}_2$.

   (b) Deduce that P has no factor of degree 1 in $\mathbf{Z}_2[X]$.

   (c) Enumerate all polynomials of degree 2 in $\mathbf{Z}_2[X]$ and identify the one $Q(X)$ which is irreducible.

   (d) Show that $Q(X)$ does not divide $P(X)$.

   (e) Deduce that $P(X)$ is irreducible.

Exercise 2 Elliptic Curves and Finite Fields

We consider the finite field $\mathbf{K} = \mathsf{GF}(7) = \mathbf{Z}_7$. As $\mathbf{K}$ is of characteristic 7, an elliptic curve $\mathrm{E}_{a,b}$ over $\mathbf{K}$ is defined by

$$\mathrm{E}_{a,b} = \{\mathcal{O}\} \cup \{(x,y) \in \mathbf{K}^2 \mid y^2 = x^3 + ax + b\}.$$

1. Compute the multiplication table of the elements of $\mathbf{K}$.

2. Find all the points of $\mathrm{E}_{2,1}$. How many points do you find? Is Hasse's Theorem verified?

3. For each point $P \in \mathrm{E}_{2,1}$, compute $-P$ and check that it lies on the curve as well.

4. To which group is $\mathrm{E}_{2,1}$ isomorphic to? Compute the addition table of $\mathrm{E}_{2,1}$.

Exercise 3 Encoding Messages in Elliptic Curves

We consider the ElGamal cryptosystem over an elliptic curve. I.e., we work over a field $\mathbf{Z}_p$, use parameters a, b to define the curve $y^2 = x^3 + ax + b$, and use a generator P of the curve, who has a prime order n. (We recall that n is close to p, due to the Hasse Theorem.) Given a secret key d, the public key is $Q = dP$. Normally, we encrypt group elements. To encrypt a point M in the curve, we compute $R = rP$ for $r \in_U \mathbf{Z}_n$ and $S = M + rQ$. The ciphertext is (R, S).

We want to encrypt bitstrings (of fixed length which is less than $\log_2 n$). To encrypt a bitstring m, we map it to a point on the elliptic curve $M = \mathsf{map}(m)$ then encrypt M. We assume that map is efficiently invertible so that after decrypting (R, S) we can apply map^{-1} to obtain m. In this exercise, we consider the problem of defining map.

1. Given the secret d and the parameters (p, a, b, n, P) recall how the above ElGamal cryptosystem is constructed from the semi-static Diffie-Hellman protocol. Then, give the method to decrypt the ciphertext (R, S).

2. One convenient way to map an element of $\mathbf{Z}_n$ to the elliptic curve is to multiple the integer by P. We define a function $\mathsf{integer}$ to convert a bitstring into an integer. I.e., $\mathsf{integer}(m) = \sum_{i=1}^{|m|} m_i 2^{|m|-i}$, where $|m|$ is the length of the bitstring m and m_i is the ith bit of m.

   List the requirements on the map function to make the cryptosystem usable.

   Say if the function $\mathsf{map}(m) = \mathsf{integer}(m)P$ satisfies them.

3. We now consider $\mathsf{map}(m) = (x, y)$ where $x = \mathsf{integer}(m)$, y is the smallest square root of $x^3 + ax + b$, and $\mathsf{integer}$ converts a bitstring into an integer. By reviewing the requirements on map, what do you think of this function?

4. Let k be a small (public) constant. We change the previous construction by taking x be the smallest integer at least equal to $2^k \mathsf{integer}(m)$ such that $x^3 + ax + b$ is a quadratic residue. Review again the required properties on map and provide algorithms to compute map and map^{-1}.

5. Assuming that p has 256 bits, propose a value (as small as possible) for k so that the previous construction should work with probability at least $1 - 2^{-80}$.

   HINT: for this question, assume that $x \mapsto x^3 + ax + b$ maps intervals of size 2^k to "random values" in $\mathbf{Z}_p$.