Advanced Cryptology - Homework

Part I: on Wiedemann's algorithm

Given a linear sequence $(s_i)_{i\in\mathbb{N}}$ of elements of a finite field K, whose minimal polynomial has degree less than d, it is possible with Berlekamp-Massey's algorithm to recover from $2d$ successive terms $(s_0, \dots, s_{2d-1})$ of the sequence its minimal polynomial. The first goal of Part I is to analyse this algorithm.

1. Suppose there exist $a_0, \dots, a_d \in K$ such that
$$a_0 s_k + a_1 s_{k+1} + \dots a_d s_{k+d} = 0 \quad \text{for any } k < d.$$
Let $\tilde{S}, P \in K[X]$ be the polynomials defined by
$$\tilde{S}(X) = u_{2d-1} + u_{2d-2}X + \cdots + u_0 X^{2d-1} \in K[X],$$
$$\text{and } P(X) = a_0 + a_1 X + \cdots + a_d X^d.$$
Show that the terms of the product $P\tilde{S}$ of degree between d and $2d-1$ are all equal to zero.
2. Deduce that there exist two polynomials $A, B \in K[X],\ \deg(A) < d,\ \deg(B) < d$, such that
$$A(X) = B(X)X^{2d} + P(X)\tilde{S}(X).$$
Show that you can recover P using the extended Euclidean algorithm applied to the polynomials X^{2d} and $\tilde{S}$ (hint: stop the algorithm as soon as you get polynomials R, U and V such as $R(X) = U(X)X^{2d} + V(X)\tilde{S}(X)$ and $\deg R < d$). What is the complexity of this computation?
3. Give an illustration of this algorithm for a linear sequence of your choice on Pari/GP.

Back to Wiedemann's algorithm with the same notations as those used in the lectures (M is a square matrix and v a vector of size n), we want to analyze the probability that given an arbitrary vector u, the minimal polynomial returned by Berlekamp-Massey for the sequence $s_i = {}^t u.M^i.v$ is not equal to the minimal polynomial of M with respect to v.

4. Let P_v be the minimal polynomial of M with respect to v and $P_1, \dots, P_k$ its irreducible factors; for $j \in \{1, \dots, k\}$, let $Q_j = P_v/P_j$.
Show that if ${}^t u.Q_j(M).v \neq 0$ for all $j \in \{1, \dots, k\}$, then the minimal polynomial of the sequence $({}^t u.M^i.v)_{i\in\mathbb{N}}$ is equal to P_v.
5. Let $j \in \{1, \dots, k\}$. Prove that the set $\{u \in K^n \mid {}^t u.Q_j(M).v = 0\}$ contains $card(K)^{n-1}$ elements.
6. Deduce that the probability that the minimal polynomial of the sequence $({}^t u.M^i.v)_{i\in\mathbb{N}}$, for u a uniformly random element in K^n, is different from P_v is smaller than $\frac{n}{card(K)}$.

Part II: space of differentials of a curve and applications to cryptography

Let $\mathcal{C}$ be an algebraic curve over a perfect field $\mathbb{K}$. We define the space of differential forms on $\mathcal{C}$ as the $\overline{\mathbb{K}}(\mathcal{C})$-vector space generated by symbols of the form dx where $x \in \overline{\mathbb{K}}(\mathcal{C})$, with the usual relations:

(i) $d(x+y) = dx + dy$,

(ii) $d(xy) = x\,dy + y\,dx$,

(iii) $da = 0$

for any $x, y \in \overline{\mathbb{K}}(\mathcal{C})$ and $a \in \overline{\mathbb{K}}$. This set is denoted $\Omega(\mathcal{C})$.
As $\mathcal{C}$ is curve, an important (admitted) fact is that $\Omega(\mathcal{C})$ has dimension 1 over $\overline{\mathbb{K}}(\mathcal{C})$. Thanks to this result, it is possible to define the divisor of a differential ω. Given $P \in \mathcal{C}$ and $t \in \overline{\mathbb{K}}(\mathcal{C})$ a uniformizer at P, then there exists a unique function $f := d\omega/dt$ such that $d\omega = f\,dt$, and we set

$$\mathrm{ord}_P(\omega) := \mathrm{ord}_P(d\omega/dt).$$

It is not very difficult to check that this definition is independant of the choice of the uniformizer t at P. As for functions, we can then define the divisor associated to $\omega \neq 0$ as

$$\mathrm{div}(\omega) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(\omega)\,(P),$$

and this sum is finite, i.e. for all but finitely many $P \in \mathcal{C}$, $\mathrm{ord}_P(\omega) = 0$ (this is also admitted).
We say that a differential $\omega \in \Omega(\mathcal{C})$ is *regular* if the associated divisor is effective, i.e. $\mathrm{div}(\omega) \geq 0$. The set of regular differentials together with 0 is denoted $\Omega^1(\mathcal{C})$.

1. What is the divisor of dx on the elliptic curve $\mathcal{E} : y^2 = (x - x_1)(x - x_2)(x - x_3)$? Deduce that $\mathrm{div}\left(\frac{dx}{y}\right) = 0$, otherwise said dx/y is a differential with no poles nor zeroes.

2. More generally, let $\mathcal{H} : y^2 = f(x) = \prod_{i=1}^{d}(x - x_i)$ be an hyperelliptic curve. Prove that

$$dx = \begin{cases} \sum_{i=1}^{d}(P_i) - 3(\mathcal{O}) \text{ if } d \text{ is odd,} \\ \sum_{i=1}^{d}(P_i) - 2(\mathcal{O}_1) - 2(\mathcal{O}_2) \text{ if } d \text{ is even,} \end{cases}$$

   where P_i stands for the point of coordinates $(x_i, 0)$ and $\mathcal{O}$ the point(s) at the infinity.

3. Show that the image in $\mathrm{Pic}(\mathcal{C})$ of the divisors of differentials on $\mathcal{C}$ are all in the same divisor class.

   We call this class the *canonical* class $[K]$ and any divisor of a differential on $\mathcal{C}$ is called a *canonical divisor* of $\mathcal{C}$.

4. Show that $\Omega^1(\mathcal{C})$ is a $\overline{\mathbb{K}}$-vector space isomorphic to $\mathcal{L}(K)$ for any canonical divisor K of $\mathcal{C}$.

We use these new notions to state a more precise version of Riemann-Roch's theorem than the one given during the lectures:

Theorem 1 (R-R (admitted))**.** *Let $\mathcal{C}$ be a smooth curve and K a canonical divisor on $\mathcal{C}$. There exists an integer $g \geq 0$ called the genus of $\mathcal{C}$, such that for any divisor $D \in Div(\mathcal{C})$,*

$$\ell(D) - \ell(K - D) = \deg D - g + 1.$$

3. Taking $D = 0$ in R-R, prove that $\Omega^1(\mathcal{C})$ has dimension g over $\overline{\mathbb{K}}$.
4. Taking this time $D = K$ in R-R, show that $\deg K = 2g - 2$ and recover the version of R-R given during the lectures.
5. Let $\mathcal{H}$ is a hyperelliptic curve with equation $y^2 = f(x)$, $\deg f = d$. Show that

$$\Omega^1(\mathcal{H}) = \left\langle \frac{dx}{y}, \frac{x\,dx}{y}, \dots, \frac{x^{\lfloor (d-1)/2-1 \rfloor} dx}{y} \right\rangle,$$

and the genus of $\mathcal{H}$ is $\lfloor (d-1)/2 \rfloor$.

Application 1: solving the DLP on anomalous curves
It is well-known that the DLP in a finite additive group is really easy: its resolution consists in computing modular division, which is easily done with the extended Euclidean algorithm. Our goal is to investigate elliptic curves defined over $\mathbb{F}_p$, p prime, for which there exists an explicit non trivial homomorphism to $(\overline{\mathbb{F}}_p, +)$.

6. Prove that if such a homomorphism exists, then $\#E(\mathbb{F}_p) = p$ (hint: use Hasse bound). These curves are called *anomalous* (or trace-1) curves.

Let $E : y^2 = f(x)$ be an anomalous elliptic curve and P be a generator of $E(\mathbb{F}_p)[p]$.

7. Prove that there exists a function f_P such that $\operatorname{div}(f_P) = p(P) - p(\mathcal{O})$. Show that the differential df_P/f_P is regular at $\mathcal{O}$ (we will admit that if a function has no pole at a given point, then its differential is regular at this point).
8. Deduce that

$$\frac{df_P}{f_P} = (a_{P,0} + a_{P,1}t + a_{P,2}t^2 + \dots)dt \tag{1}$$

where $t = x/y$ and $a_{P,i} \in \mathbb{F}_p$.
9. Show that $Q \in E(\mathbb{F}_p)[p] \mapsto df_Q/f_Q \in \Omega_{\mathbb{F}_p}(E)$, where f_Q is defined as above, is an injective group homomorphism. Deduce that the map $Q \in E(\mathbb{F}_p)[p] \mapsto a_{Q,0} \in \mathbb{F}_p$ is also a group morphism (we will assume that it is injective).
10. Let $f_Q = b_{Q,0}t^{-p} + b_{Q,1}t^{-p+1} + \dots$ be the series expansion of f_Q at $\mathcal{O}$ with respect to t. Show that $a_{Q,0} = -b_{Q,1}/b_{Q,0}$.
11. Using Miller's algorithm to compute the series expansion of f_P, write down a program in Pari/GP that allows to solve the DLP on the elliptic curve[1] $E : y^2 = x^3 + ax + b$ defined over $\mathbb{F}_p$ where

$$a = 425706413842211054102700238164133538302169176474,$$

[1] If you want to know how this curve has been obtained, read the paper *Generating Anomalous Elliptic Curves* by Leprévost et al.

$$b = 20336293654882693667326444498286633995326553016 6$$

and

$$p = 73075081866545145911259690563843304823206747172 3.$$

Test it with the points $P = (3, 6924580356122950180928565860844766714121236172 08)$ and $Q = (4, 3364098639847824116734502424632911780695700603 24)$.

Application 2: canonical models for genus 2 curves
Let χ be a curve of genus 2.

13. Show that there exist functions $x, y \in \mathbb{K}(\chi)$ such that $\mathcal{L}(K) = \langle 1, x \rangle$ and $\mathcal{L}(3K) = \langle 1, x, x^2, x^3, y \rangle$. Determine all the polynonials in x and y belonging to $\mathcal{L}(6K)$.
14. Using the Riemann-Roch theorem, compute the dimension of $\mathcal{L}(6K)$.
15. Deduce a map from χ to an hyperelliptic curve of genus 2 in the plane. This shows in particular that every genus 2 curve is hyperelliptic.