Homework 13 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

31.01.2012

Exercise 36.

Consider a polynomial in $x \in \mathbb{R}$ of degree n and its first derivative:

$$f(x) = f_n x^n + \cdots + f_0, \quad f'(x) = n f_n x^{n-1} + \cdots + f_1.$$

The *discriminant* Δ is an invariant to evaluate the number and multiplicity of roots in a polynomial $f(x)$. It is computed as following:

$$\Delta = (-1)^{\binom{n}{2}} \mathrm{Res}(f, f') \frac{1}{f_n}.$$

The *resultant* $\mathrm{Res}(f,g)$ is used to compute shared roots in the polynomial $f(x)$ of degree n and polynomial $g(x)$ of degree m. The resultant is defined as the determinant of the $(m+n) \times (m+n)$ *Sylvestermatrix*:

$$\mathrm{Res}(f,g) = \det \begin{pmatrix} f_n & & \cdots & & f_0 & 0 & & 0 \\ 0 & f_n & & \cdots & & f_0 & & \\ & & \ddots & & & & \ddots & 0 \\ 0 & & 0 & f_n & & \cdots & & f_0 \\ g_m & & \cdots & & g_0 & 0 & & 0 \\ 0 & g_m & & \cdots & & g_0 & & \\ & & \ddots & & & & \ddots & 0 \\ 0 & & 0 & g_m & & \cdots & & g_0 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \end{matrix}$$

(a) Compute the discriminant Δ of the quadratic polynomial $f(x) = ax^2 + bx + c$.

(b) Compute the discriminant Δ of the cubic polynomial $f(x) = x^3 + ax + b$.

Exercise 37.

Describe how the DSA signature scheme can be carried out in a group of $\mathbb{F}_p$-rational points on an elliptic curve $E/\mathbb{F}_p$.