Lehrstuhl für
Theoretische Informationstechnik

RWTH RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

Homework 8 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten

03.07.2008

Exercise 20. Create a Challenge-Response protocol in which Alice and Bob authenticate each other. The protocol shall be based on Public-Key cryptography. Is it possible to reach this goal without a hash function in just 3 messages?

Excercise 21. Consider the equation

$$Y^2 = X^3 + X + 1.$$

Show that this equation describes an elliptic curve over the field $\mathbb{F}_7$.

a) Determine all points in $E(\mathbb{F}_7)$ and compute the trace t of E.

b) Show that $E(\mathbb{F}_7)$ is cyclic and give a generator.

Excercise 22. Let $E : Y^2 = X^3 + aX + b$ be a curve over the field K with $\mathrm{char}(K) \neq 2, 3$ and let $f := Y^2 - X^3 - aX - b$.
A point $P = (x, y) \in E$ is called *singular*, if both formal partial derivatives $\partial f/\partial X(x, y)$ and $\partial f/\partial Y(x, y)$ vanish at P.
Prove that for the discriminant Δ of E it holds that

$$\Delta \neq 0 \Leftrightarrow E \text{ has no singular points.}$$