htw saar

Studiengang Kommunikationsinformatik (Master)
Studiengang Praktische Informatik (Master)
Prof. Dr.–Ing. Damian Weber

Sicherheit und Kryptographie – Übung

Aufgabe 1 (Elliptische Kurven)

Gegeben sei die elliptische Kurve

$$E: \quad y^2 \equiv x^3 - x + 3 \ mod\ 7.$$

a) Überprüfen Sie mittels

$$4a^3 + 27b^2 \not\equiv 0 \ mod\ 7$$

die korrekte Parameterwahl.

b) Finden Sie alle 6 Punkte von E.

c) Finden Sie einen Punkt der Ordnung 2 auf E.

d) Stellen Sie die Verknüpfungstabelle von $(E, +)$ auf.

e) Finden Sie einen Punkt der Ordnung 3 auf E.

f) Finden Sie einen Punkt P der Ordnung 6 auf E.

g) Führen Sie das Diffie–Hellman–Protokoll mit Hilfe von P aus.
Alice wählt hierbei als geheimen Multiplikator $a = 5$ und Bob $b = 2$.