Prof. Dr. M. Kreuzer
P. Ackermann

Abgabe: 04.07.2005, 14h

Kryptografie
Übungsblatt 11

Aufgabe 32:
Sei $K = \mathbb{F}_p$ mit $p = 751$ und die elliptische Kurve $E(K)$ sei definiert durch $y^2 + y = x^3 - x$. Die Kurve $\overline{E}(K)$ hat 727 Punkte. Die Klartexteinheiten seien die Ziffern 0 bis 9 sowie die den Buchstaben A bis Z entsprechenden Zahlen 10 bis 35. Sei $\kappa = 20$.

a) Benutzen Sie die Methode aus Bemerkung 4.17, um die Nachricht „STOP007“ als Folge von sieben Punkten auf $\overline{E}(K)$ darzustellen.

b) Übersetzen Sie die Punkte $(484, 214)$, $(401, 222)$ in eine Textnachricht.

c) Sei $P = (0, 0)$. Benutzen Sie das elliptische ElGamal-Kryptosystem, um die Nachricht aus a) zu verschlüsseln. Der öffentliche Schlüssel des Empfängers sei der Punkt $(201, 380)$, die Folge der zufälligen k's sei $386, 209, 118, 589, 312, 483, 335$.

d) Simulieren Sie den Austausch obiger Nachricht mit Hilfe des elliptischen Massey–Omura–Kryptosystems, wobei der geheime Schlüssel von A gleich 13 und der von B gleich 35 sei.

8 Punkte