Technische Universität Braunschweig

Institut für Theoretische Informatik

Dr. Jürgen Koslowski

Cryptologie 3

Aufgabenblatt 4, 2017-05-29

Aufgabe 1 [10 PUNKTE]

Gegeben ist die Primzahl $p = 181$ und die elliptische Kurve $y^2 = x^3 - x$.

(a) [4 PUNKTE] Bestimmen Sie die Zahl $N = \#E(\mathbb{Z}_p)$.

(b) [4 PUNKTE] Beweisen oder widerlegen Sie, daß $E(\mathbb{Z}_p)$ eine zyklische Untergruppe mit mindestens 20 Elementen hat.

Aufgabe 2 [10 PUNKTE]

Es sei E die elliptische Kurve $y^2 = x^3 + x + 13$ über $\mathbb{Z}_{31}$. Es ist $\#E(\mathbb{Z}_{31}) = 34$ und außerdem ist $(9, 10)$ ein Element der Ordnung 34 in $E(\mathbb{Z}_{31})$.

Das *Menezes-Vanstone-Kryptosystem* über E hat als Klartextraum $\mathbb{Z}_{31}^* \times \mathbb{Z}_{31}^*$. Es sei $x_A = 25$ der geheime Exponent von Alice.

(a) [4 PUNKTE] Schreiben Sie ein allgemeines Programm, mit dem man die Summen

$$i \cdot (x, y)$$

mit $i \in \mathbb{N}$ und $(x, y) \in E(\mathbb{Z}_{31})$ berechnen kann. Hinweis: schnelle "Exponentiation".

Berechnen Sie damit den öffentlichen Schlüssel y_A.

(b) [4 PUNKTE] Entschlüsseln Sie den folgenden Chiffretext aus Tripeln (y_B, b_0, b_1):

$$(((4, 9), 28, 7), ((19, 28), 9, 13), ((5, 22), 20, 17), ((25, 16), 12, 27))$$

(c) [2 PUNKTE] Jeder Klartextwert repräsentiert zwei Buchstaben des Alphabetes. Finden Sie das Klartextwort!

Hinweis: Es handelt sich um ein englisches Wort. Beachten Sie, das hier die folgende Korrespondenz $A \leftrightarrow 1, \ldots, Z \leftrightarrow 26$ gilt.

Besprechung Montag, 2017-06-12, 11:30 in der Übung