Übungen zur Vorlesung Kryptologie
Prof. Dr. Klaus Reinhardt / Dr. Bernd Borchert

WS 2013/14
Universität Tübingen
24.1.2014

9. Übungsblatt

Aufgabe 1.
Berechne den diskreten Logarithmus von 53 zur Basis 2 modulo 61 mit dem Pohlig-Hellman Algorithmus.

Aufgabe 2
Sei $n = pq$ mit p, q prim. Wie können diskrete Logarithmen modulo n berechnet werden? Gibt es immer eine Lösung? Ist diese immer eindeutig?

Aufgabe 3.
Berechne den diskreten Logarithmus von 24 zur Basis 2 modulo 97 mit der Index-Calculus Methode.

Aufgabe 4.
Welche Bits des diskreten Logarithmus modulo 10009 können leicht berechnet werden? Wie lauten diese im Fall des diskreten Logarithmus von 17 zur Basis 11 ?

Aufgabe 5.
Das verallgemeinerte ElGamal Public-key Kryptosystem werde mit der Gruppe $(\mathbb{Z}_n, +)$ verwendet. Wie würde ein Algorithmus (Pseudocode) aussehen, der das System bricht, also ohne Kenntniss des geheimen Schlüssels entschlüsseln kann

Aufgabe 6
Welche Polynome in $\mathbb{Z}_3[x]$ vom Grad 3 sind irreduzibel?

Aufgabe 7
Was geht schief, wenn versehentlich modulo eines reduziblen Polynoms $f(x)$ gerechnet wird?

Aufgabe 8.
Aus welchen Punkten besteht die elliptische Kurve E mit $p = 13, a = 2, b = 3$?

Aufgabe 9.
Sei sei E wie in letzter Aufgabe, $\alpha = (0, 4)$ und $a = 7$ der geheime Exponent. Ver- und entschlüssle die Nachricht $x = (6, 7)$ mit $k = 3$ mit ElGamal.

Aufgabe 10.
Sei sei E, α und a wie in letzter Aufgabe. Ver- und entschlüssle die Nachricht $x = (11, 11)$ mit dem Menezes-Vanstone Kryptosystem.