Zahlentheorie und Kryptologie, Wintersemester 2012/13
M. Hortmann

Blatt 1

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen								**Gruppe**	**Tutor**
1a	b	2a	b	c	3a	b	c	**Summe**	**bearbeitet**
1	1	1	1	1	1	1	1	8 Punkte=100%	

Aufgabe 1
Zeigen Sie:
a) Ist 2^n-1 eine Primzahl, so ist n ebenfalls eine Primzahl.
b) Ist 2^n+1 eine Primzahl, so ist n eine Potenz von 2.

Aufgabe 2
Lineare Schieberegisterfolgen:
Sei K ein Körper und $a=(a_0,\ldots,a_{n-1})\in K^n$. Ist dann $x=(x_0,\ldots,x_{n-1})\in K^n$, so erhält man mit der Rekursion $x_{n+k}:=\sum_{i=0}^{n-1} a_i x_{i+k}$ die lineare Schieberegisterfolge (x_i) in K. Die lineare Abbildung $(x_0,\ldots,x_{n-1})\mapsto(x_1,\ldots,x_n)$ wird offenbar durch die Matrix $A=\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \ldots & 1 \\ a_0 & a_1 & a_2 & \ldots & a_{n-1} \end{pmatrix}$
beschrieben.

a) Man berechne das charakteristische Polynom dieser Matrix.

b) Ist K ein endlicher Körper mit $|K|=q$, so nennt man ein Polynom $f\in K[X]$ vom Grad $n\geq 2$ primitiv, wenn es irreduzibel ist und wenn im Restklassenkörper $F=K[X]/<f>$ das Element $\overline{X}$ die multiplikative Gruppe des Körpers erzeugt, also die Ordnung q^n-1 besitzt.

Man zeigt leicht, daß ein Polynom genau dann primitiv ist, wenn ggT(X,f)=1 und das Element $\overline{X}$ in der multiplikativen Gruppe des Restklassenrings $K[X]/<f>$ die Ordnung q^n-1 besitzt. Setzen Sie dies voraus, um zu zeigen, daß das Polynom $X^7+X+1\in\mathbb{Z}_2[X]$ primitiv ist.

c) In der Vorlesung wurde gezeigt, daß eine mit dem Kontrollvektor $(a_0,\ldots a_{n-1})\in K^n$ erzeugte lineare Schieberegisterfolge maximale Länge besitzt, wenn das Polynom $a_0+a_1X+\ldots+a_{n-1}X^{n-1}+X^n$ primitiv ist. Schreiben Sie Programmcode in Pari oder Sage[1], welche ausgehend vom Kontrollvektor *a*=(1,1,0,0,0,0,0) und dem Startvektor $x=(x_0,\ldots,x_6)=(0,0,0,0,0,0,1)$ eine lineare Schieberegisterfolge erzeugt. Lt. b) hat diese die Periode 127. Produzieren Sie den Bitstring $(x_0,\ldots,x_{253})$, also genau zwei Perioden.

Aufgabe 3

a) Sei $g:\mathbb{Z}_2^n\to\mathbb{Z}_2^n$ eine beliebige Abbildung.
Zeigen Sie, daß die Abbildung $f:\mathbb{Z}_2^n\times\mathbb{Z}_2^n\to\mathbb{Z}_2^n\times\mathbb{Z}_2^n$, gegeben durch $(x,y)\mapsto(y,\ x+g(y))$, bijektiv ist. Geben Sie die inverse Abbildung konkret an.

b) Wir können Elemente von $x=(x_0,\ldots,x_{n-1})\in\mathbb{Z}_2^{2n}$ auffassen als Zahlen $\sum_{i=0}^{n-1}x_i2^i$. Das Quadrat einer solchen Zahl läßt sich auffassen als Bitstring der Länge 4*n*. Von diesem Ergebnis betrachten wir die mittleren 2*n* Bit. Ingesamt haben wir damit eine nicht-lineare Abbildung $g:\mathbb{Z}_2^{2n}\to\mathbb{Z}_2^{2n}$. Gehen wir aus von *n*=64, so erhalten wir eine Abbildung $g:\mathbb{Z}_2^{128}\to\mathbb{Z}_2^{128}$ und mit der Konstruktion aus a) eine bijektive Abbildung $f:\mathbb{Z}_2^{256}\to\mathbb{Z}_2^{256}$.

Sei $F:=\underbrace{f\circ\ldots\circ f}_{32-\text{mal}}$. Verwandeln Sie den Text "Die Aufgabe ist recht aufwaendig", der aus genau 32 Zeichen inklusive Leerzeichen besteht, via Ascii-Code in einen Bitstring $x\in\mathbb{Z}_2^{256}$.

Berechnen Sie *y*=*F*(*x*) und geben diesen String als Hex-String aus.
Freiwilliger Zusatz: Berechen Sie $z=F^{-1}(y)$ und zeigen Sie, daß *z*=*x*.

1 Sie können online rechnen auf www.sagenb.org