Zahlentheorie und Kryptologie, Wintersemester 2012/13
M. Hortmann

Blatt 4

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen							**Gruppe**	**Tutor**
1	b	c	d	2a	b	3	**Summe**	**bearbeitet**
1	1	1	1	1	1	1	5 Punkte=100%	

Aufgabe 1

a) Sei $p \in \mathbb{N}$ eine Primzahl. Begründen Sie, warum es ein irreduzibles Polynom vom Grad 2 in $\mathbb{Z}_p[X]$ geben muß und daher einen Körper mit p^2 Elementen.

Ist K ein Körper mit p^2 Elementen, so enthält er in natürlicher Weise $\mathbb{Z}_p$ als Teilkörper. Der Frobenius-Automorphismus $\sigma : K \to K$, ist durch $x \mapsto x^p$ gegeben.

b) Man zeige: $\mathbb{Z}_p$ ist der Fixkörper von σ, d.h. $\mathbb{Z}_p = \{x \in K \mid \sigma(x) = x\}$ und es gilt auch $\sigma \circ \sigma = \mathrm{id}_K$.

c) Die Norm eines Elements $x \in K$ wird definiert durch $N(x) := x \cdot \sigma(x)$.
Wieso ist $\forall\, x \in K : N(x) \in \mathbb{Z}_p$?

d) Offenbar ist die Abbildung $K^* \to \mathbb{Z}_p^*$, $x \mapsto N(x)$ ein Gruppenhomomorphismus.
Zeigen Sie, daß dieser surjektiv ist.
(Man könnte benutzen, daß die multiplikative Gruppe eines endlichen Körpers zyklisch ist.).

Aufgabe 2
Der österreichische Briefbombenattentäter Franz Fuchs hatte dummerweise angenommen, es würde mehrere Wochen dauern, eine auf der Basis des RSA-Moduls *n*=
630548215070129547156718332495889632234434145411971275888376987603
260225252787926135276738944105689100036295535868141424386536403649
578707699128189491432138631900590774729214990015369102760964884776
344849717811484309528915040117952098061886881
verschlüsselte Nachricht zu entschlüsseln.
Dabei findet man einen Faktor von *n* schon mit der einfachsten Version der Fermat-Faktorisierung!

a) Wie also lautet die Primfaktorzerlegung von *n*?

b) Franz Fuchs hatte als öffentlichen Exponenten die Zahl *e*=
`508075310835159009812633969174411123496728859672737076695139826186`
`257647581337481521676692825102982808222076238747753504407`
gewählt, und die erste Zeile seiner verschlüsselten Botschaft sah so aus *c*=
`463316335616613937318842101415083702006628892795168389554894402706`
`884035322375721126316678871052346087047872057770161604068825594947`
`480777575090664841774749749032122958886916388656231305149413112661`
`671360620310298582755616480043108904735117491`

Finden Sie die Zahl $t \in \mathbb{Z}_n$, für die gilt $t^e = c$.
Wenn sie *t* als Dezimalzahl nehmen, interpretieren Sie jede 3-Zifferngruppe als Ascii-Code.
Wie lautete demnach die erste Zeile von Fuchsens Botschaft?

Aufgabe 3 Fermat-Faktorisierung mit Faktorbasis:

Betrachten Sie die Zahl *n*=48202631.

Nehmen Sie als Faktorbasis $B = \{p_1, p_2, p_3, p_4, p_5\} = \{2,3,5,7,11\}$.
Wählen Sie solange zufällige Elemente $x \in \mathbb{Z}_n$, bis Sie 8 gefunden haben, für die x, als natürliche Zahl interpretiert, größer als $\sqrt{n}$ ist und für die $z = x^2$, interpretiert als natürliche Zahl, in der Faktorbasis aufgeht.

Wir haben dann also $z_i = 2^{\alpha_{1,i}} \cdot 3^{\alpha_{2,i}} \cdot 5^{\alpha_{3,i}} \cdot 7^{\alpha_{4,i}} \cdot 11^{\alpha_{5,i}}$ für $i = 1, \ldots, 8$.
Man bilde jetzt eine Matrix $A = (a_{j,i})$ mit 5 Zeilen und 8 Spalten und Koeffizienten in $\mathbb{Z}_2$. Dabei sei $a_{j,i} = 0$, falls $\alpha_{j,i}$ gerade und $a_{j,i} = 1$, falls $\alpha_{j,i}$ ungerade. Man finde jetzt mehrere Vektoren $\lambda \in \mathbb{Z}_2^8$ mit $A\lambda = 0$. Für ein solches λ berechne man $\prod_{i=1}^{8} z_i^{\lambda_i} = \prod_{j=1}^{5} p_j^{\sum_{i=1}^{8} \alpha_{j,i}\lambda_i}$. Nun ist $\beta_j = \sum_{i=1}^{8} \alpha_{j,i}\lambda_i$ gerade.
Setzt man $y = \prod_{j=1}^{5} p_j^{\beta_j/2}$ und $x = \prod_{i=1}^{8} x_i^{\lambda_i}$, so folgt $x^2 = y^2$ als Gleichung in $\mathbb{Z}_n$.

Man benutze diese Gleichung zur Faktorisierung von *n*, ggf. durch Zuhilfenahme weiterer Lösungen λ der Gleichung $A\lambda = 0$.