Mathematische Grundlagen der Kryptografie (1321) SoSe 05

Klausur am 20.08.2005:

Lösungsvorschläge zu den Aufgaben

zu Aufgabe I.1

(a) Das Wort HALLO mit der Caesar-Verschiebung und dem Schlüssel 5 verschlüsselt ist MFQQT.

(b) Das Wort HALLO verschlüsselt mit dem Permutationskryptosystem und dem Schlüssel SILKE und dem Schlüsselbuchstaben H ist STEEC.

(c) Das Wort HALLO mit dem affinen Kryptosystem und dem Schlüssel $(a, b) = (3, 5)$ verschlüsselt ist AFMMV.

zu Aufgabe I.2

Die primitiven Elemente von $\mathbb{F}_{11}$ sind $2, 8, 7, 6$.

zu Aufgabe I.3

Der Grad des Minimalpolynoms von $\sqrt{1+\sqrt{3}}$ ist 4.

zu Aufgabe I.4

Eine elliptische Kurve mit $72 = 2^3 \cdot 3^2$ Elementen kann folgende Struktur haben: $\mathbb{Z}/72\mathbb{Z}$ oder $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$ oder $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ oder $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

zu Aufgabe I.5

Der Satz von Lagrange lautet folgendermaßen: Sei G eine endliche Gruppe und H eine Untergruppe. Dann gilt $|G| = [G : H] \cdot |H|$.

zu Aufgabe II.1

Der Text DPYDBLUZJOLUPOULUCPLSLYMVSNPUKLYRSHBZBY ist mit der Caesar-Verschiebung verschlüsselt.

Behauptung Der Klartext lautet WIR WUENSCHEN IHNEN VIEL ERFOLG IN DER KLAUSUR.

Beweis Da die Caesar-Verschiebung ein monoalphabetisches Kryptosystem ist, hilft hier eine Häufigkeitsanalyse der Buchstaben:

Buchstabe	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Häufigkeit	-	3	1	2	-	-	-	1	-	1	1	6	1	1	2	4	-	1

S	T	U	V	W	X	Y	Z
3	-	5	1	-	-	4	2

Der häufigste Buchstabe ist also das L. Die Vermutung liegt nahe, dass das L dem E entspricht, bzw. die 11 der 4. Damit wäre der Schlüssel dann 7 und die Verschlüsselungsabbildung

Klartext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Geheimtext	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

R	S	T	U	V	W	X	Y	Z
Y	Z	A	B	C	D	E	F	G

Damit ist der Klartext WIRWUENSCHENIHNENVIELERFOLGINDERKLAUSUR oder WIR WUENSCHEN IHNEN VIEL ERFOLG IN DER KLAUSUR.

zu Aufgabe II.2

Wir beschreiben das Diffie-Hellman-Schlüsselaustauschsystem über elliptischen Kurven:

(a) Gegeben sei eine elliptische Kurve $E(a, b, \mathbb{K})$. Der öffentliche Schlüssel ist ein Punkt S auf der Kurve, der eine möglichst große Untergruppe der Kurve erzeugt. Optimal ist eine elliptische Kurve, die zyklisch ist, und S ist ein erzeugendes Element.

(b) Alice wählt zufällig eine natürliche Zahl e_A und berechnet $e_A S$. Bob wählt ebenfalls zufällig eine natürliche Zahl e_B und berechnet $e_B S$.

(c) Der gemeinsame (geheime) Schlüssel ist $e_A e_B S$.

(d) Die Sicherheit des Systems beruht zum einen auf der Annahme, dass das diskreter Logarithmus Problem über elliptischen Kurven schwer zu lösen ist. Zum zweiten beruht die Sicherheit auf der Annahme, dass das diskreter Logarithmus Problem gelöst werden muss, um das Diffie-Hellman-System zu brechen.

zu Aufgabe II.3

Sei $L = \{x \in \mathbb{Z}^3 \mid x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \text{ mit } x_1 \equiv x_2 (\text{mod} 3) \text{ und } x_1 \equiv x_3 (\text{mod} 4)\}$.

(a) **Behauptung** Die Menge L ist ein Gitter mit Basis $\left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 4 \end{pmatrix} \right)$.

Beweis Sei $x \in L \left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 4 \end{pmatrix} \right)$. Dann gibt es $a_1, a_2, a_3 \in \mathbb{Z}$ mit $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = a_1 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix} + a_3 \begin{pmatrix} 0 \\ 0 \\ 4 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_1 + 3a_2 \\ a_1 + 4a_3 \end{pmatrix}$. Also folgt $x_1 \equiv x_2 (\text{ mod } 3)$ und $x_1 \equiv x_3 (\text{mod} 4)$, das heißt, $x \in L$.

Sei nun $x \in L$, das heißt, $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ mit $x_1 \equiv x_2 (\text{mod} 3)$ und $x_1 \equiv x_3 (\text{mod} 4)$. Dann gibt es also $a_2, a_3 \in \mathbb{Z}$ mit $x_2 = x_1 + 3a_2$ und $x_3 = x_1 + 4a_2$. Damit ist $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_1 + 3a_2 \\ x_1 + 4a_2 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix} + a_3 \begin{pmatrix} 0 \\ 0 \\ 4 \end{pmatrix} \in L \left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 4 \end{pmatrix} \right)$.

Damit folgt $L = L \left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 4 \end{pmatrix} \right)$ und L ist ein Gitter mit Basis $\left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 4 \end{pmatrix} \right)$.

(b) **Behauptung** Es gilt $\det(L) = 12$.

Beweis Es ist $\det(L) = \det \begin{pmatrix} 1 & 0 & 0 \\ 1 & 3 & 0 \\ 1 & 0 & 4 \end{pmatrix} = 12.$ □

zu Aufgabe II.4

Sei q eine Primpotenz.

Behauptung Jedes quadratische Polynom aus $\mathbb{F}_q[T]$ zerfällt über $\mathbb{F}_{q^2}$ in Linearfaktoren.

Beweis Sei $f \in \mathbb{F}_q[T]$. Hat f eine Nullstelle über $\mathbb{F}_q$, dann zerfällt f schon in Linearfaktoren, denn f ist vom Grad zwei. Damit zerfällt dann f natürlich auch über $\mathbb{F}_{q^2}$ in Linearfaktoren.

Hat f keine Nullstelle, dann ist f schon irreduzibel über $\mathbb{F}_q$, denn f ist ja quadratisch. Dann ist $\mathbb{F}_q[T]/(f) = \mathbb{F}_{q^2}$ ein Körper, und f hat über diesem Körper eine Nullstelle, nämlich $[T]$. Da f quadratisch ist, zerfällt f dann schon in Linearfaktoren. □

zu Aufgabe II.5

(a) Sei p eine Primzahl, $a \in \mathbb{Z}$ mit $p \nmid a$. Sei $a^{-1} \in \mathbb{Z}$ mit $aa^{-1} \equiv 1 \bmod p$.

Behauptung $(\frac{a^{-1}}{p}) = (\frac{a}{p})$.

Beweis Es gilt $aa^{-1} \equiv 1 (\mathrm{mod} p)$, also $1 = (\frac{1}{p}) = (\frac{aa^{-1}}{p}) = (\frac{a}{p})(\frac{a^{-1}}{p})$. Damit folgt $(\frac{a^{-1}}{p}) = (\frac{a}{p})^{-1}$. Da $(\frac{a}{p}) = \pm 1$ gilt, folgt schon $(\frac{a^{-1}}{p}) = (\frac{a}{p})$. □

(b) Sei p eine Primzahl und $a, b \in \mathbb{Z}$.

Behauptung Es gilt $(\frac{a}{p}) = (\frac{b}{p})$ genau dann, wenn es ein $z \in \mathbb{Z}$ mit $z \neq 0$ und $a \equiv bz^2 (\mathrm{mod} p)$ gibt.

Beweis Es gelte $(\frac{a}{p}) = (\frac{b}{p})$. Ist $(\frac{a}{p}) = (\frac{b}{p}) = 0$, dann ist $a \equiv b \equiv 0 (\mathrm{mod} p)$, und wir können $z = 1$ wählen. Sei nun also $(\frac{a}{p}) = (\frac{b}{p}) = \pm 1$. Dann ist b invertierbar in $\mathbb{Z}/p\mathbb{Z}$. Sei $b^{-1} \in \mathbb{Z}$ mit $bb^{-1} \equiv 1 (\mathrm{mod} p)$. Mit Teil (a) gilt:

$$1 = (\frac{a}{p})^2 = (\frac{a}{p})(\frac{b}{p}) = (\frac{a}{p})(\frac{b^{-1}}{p}) = (\frac{ab^{-1}}{p}).$$

Das Element $ab^{-1} \bmod p$ ist also ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$. Damit gibt es ein $z \in \mathbb{Z} \setminus \{0\}$ mit $ab^{-1} \equiv z^2 (\mathrm{mod} p)$ oder $a \equiv bz^2 (\mathrm{mod} p)$.

Es gelte nun $a \equiv bz^2 (\mathrm{mod} p)$ für ein $z \in \mathbb{Z} \setminus \{0\}$. Ist b nicht invertierbar mod$p$, dann folgt $b \equiv 0 (\mathrm{mod} p)$ und damit auch $a \equiv 0 \bmod p$. Also $(\frac{a}{p}) = (\frac{b}{p}) = 0$. Ist b invertierbar mod$p$ mit Inversem $b^{-1} \in \mathbb{Z}$, dann ist $ab^{-1} \equiv z^2 (\mathrm{mod} p)$, also $ab^{-1} \bmod p$ ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$. Es folgt

$$1 = (\frac{ab^{-1}}{p}) = (\frac{a}{p})(\frac{b^{-1}}{p}) = (\frac{a}{p})(\frac{b}{p})$$

mit Teil (a). Dann ist aber $(\frac{a}{p}) = (\frac{b}{p})$. □

zu Aufgabe II.6

Behauptung Wenn man mit dem RSA-Verfahren eine Nachricht n zweimal verschlüsselt und zwar mit den öffentlichen Schlüsseln (m, e) und (m, f), und wenn $\mathrm{ggT}(e, f) = 1$ gilt, dann kann man den Klartext n aus den beiden Schlüsseltexten $c_e = n^e \bmod m$ und $c_f = n^f \bmod m$ berechnen.

Beweis Es gilt $\mathrm{ggT}(e, f) = 1$, also gibt es $x, y \in \mathbb{Z}$ mit $xe + yf = 1$. Wir berechnen also $c_e^x c_f^y \equiv (n^e)^x (n^f)^y \equiv n^{xe+yf} \equiv n^1 \equiv n (\mathrm{mod} m)$. □