Abgabe: 26. April 2010

Aufgabe 1. (8 Punkte)

Finden Sie zum unten stehenden Schlüsseltext den englischen Klartext und geben Sie die dabei bekannt gewordenen Teile des (monoalphabetischen) Substitutionsschlüssels an. Geben Sie in der Lösung neben dem Schlüssel auch an, in welcher Reihenfolge Sie auf die einzelnen Teile des Schlüssels gekommen sind, und welche Überlegungen Sie dazu geführt haben. (Der Klartext braucht nicht auf dem Lösungszettel erscheinen.)

```
Ague jenoa nsg--reweo uirm fgb lgrs voeyiaelj --fnwirs little go rg ugrej ir
uj vhoae, nrm rgtfirs vnotiyhlno tg irteoeat ue gr afgoe, I tfghsft I bghlm
anil ncght n little nrm aee tfe bnteoj vnot gp tfe bgolm. It ia n bnj I fnwe gp
moiwirs gpp tfe avleer, nrm oeshlntirs tfe yioyhlntigr. Bfereweo I pirm ujaelp
sogbirs soiu ncght tfe ughtf; bfereweo it ia n mnuv, moiddlj Rgweuceo ir uj
aghl; bfereweo I pirm ujaelp irwglhrtnoilj vnhairs cepgoe ygppir bnoefghaea,
nrm coirsirs hv tfe oeno gp eweoj phreonl I ueet; nrm eaveyinllj bfereweo uj
fjvga set ahyf nr hvveo fnrm gp ue, tfnt it oeqhioea n atogrs ugonl voiryivle
tg voewert ue pogu meliceontelj atevvirs irtg tfe atoeet, nrm uetfgmiynllj
krgykirs vegvle'a fnta gpp--tfer, I nyyghrt it fisf tiue tg set tg aen na aggr
na I ynr.
```

Hinweis: Verfahren Sie analog zum Vorlesungsbeispiel mittels einer Häufigkeitsanalyse der 1-*,* 2- *und* 3-*Gramme. Die dazu nötigen Tabellen finden Sie ebenso wie den Schlüsseltext auf der Webseite. Satz- und Sonderzeichen wurden nicht substituiert. Geeignete Hilfsmittel sind die "Suchen und Ersetzen"-Funktion ihres Editors oder die "Manuelle Analyse" von* `CrypTool`*.*

Aufgabe 2. (8 Punkte)

Recherchieren Sie entsprechende Häufigkeitstabellen für die deutsche Sprache. Überlegen Sie sich aufgrund dieser Daten eine Strategie und entschlüsseln den untenstehenden Ciphertext, der durch (monoalphabetische) Substitution aus einem deutschen Klartext gewonnen wurde. Geben Sie die gewonnenen Schlüsselteile, die Überlegungen zu ihrer Strategie, und ausserdem die Quelle ihrer Daten an.

```
wbo buvlph rzwb nhbob eohgyvtrq uvrqy cd guhrgbu lbnbtbu qhbyybu wvb movyvtrqbu
goxeyzloheqbu uvrqyt dbmbo wbu ibotrqkdbttbkdulteozcbtt lbndtty
```

Hinweis: Leerzeichen wurden nicht substituiert. Den Schlüsseltext finden Sie zusätzlich auf der Webseite.

Abgabe: 3. Mai 2010

Aufgabe 1. (6 Punkte)

Der Ciphertext zu dieser Aufgabe (zu finden auf der Webseite) wurde aus einem englischen Klartext durch eine Spalten-Permutation einer 9-spaltigen Matrix gewonnen. Erläuterung: Der Klartext wurde *zeilenweise* in die Matrix eingetragen und nach der Spalten-Permutation *spaltenweise* ausgelesen.

Bestimmen Sie mittels Häufigkeitsanalyse die verwendete Permutation, also ein Element von S_9. Hierfür ist ein Programm zu schreiben, vorzugsweise in `PYTHON`, dass es erlaubt, zwei beliebige Spalten aus der Matrix zu extrahieren und die Häufigkeiten der Bigramme zu zählen, die durch die Zeilen der entstehenden 2-spaltigen Matrix dargestellt werden. Das Beispiel-Programm auf der Webseite zeigt, wie man in `PYTHON` den Geheimtext einliest und in Spalten zerlegt.

Als schriftliche Lösung ist neben der gesuchten Permutation auch die Strategie und die Reihenfolge anzugeben, in der die Permuation gefunden wurde. Beim Vorrechnen ist der Programmtext anzuschreiben und zu erläutern.

Aufgabe 2. (6 Punkte)

Wir betrachten eine Verschlüsselung durch Kombination von Permutation und Substitution, d.h. die Verschlüsselungsabbildung ist von der Form $T \circ S$, wobei S eine (monoalphabetische) Substitution und T eine Permutation beschreibt.

a) Beweisen Sie, dass eine mehrfache Kombination der Form $T_n \circ S_n \circ T_{n-1} \circ S_{n-1} \circ \ldots T_1 \circ S_1$ keine zusätzliche Sicherheit im Vergleich zur einfachen Kombination $T \circ S$ bietet, egal welches Sicherheitsmodell zugrunde gelegt wird.

b) Führen Sie anhand des Beispiels auf der Webseite vor, dass diese Art von Kryptosystem nicht die Sicherheitseigenschaft IND bei einem ciphertext-only Angriff bietet. Ordnen Sie dazu den gegebenen Geheimtext einem der 5 Klartexte zu. Erläutern Sie ihre Vorgehensweise.

c) (freiwillig) Entschlüsseln Sie den als Krypto-Challenge No. 2 gegebenen Geheimtext.

Wurde zu b) ein Programm verwendet, so ist dieses beim Vorrechnen anzuschreiben und zu erläutern.

Aufgabe 3. (4 Punkte)

Wir betrachten den probabilistischen Algorithmus, der wiederholt einen Würfel als Zufallsquelle befragt, solange bis dieser eine 6 liefert. Dann bricht der Algorithmus ab. Beweisen Sie, dass der Erwartungswert der Laufzeit 6 beträgt.

Aufgabe 4. (4 Punkte)

Es sei $F : M \rightsquigarrow N$ eine surjektive mehrdeutige Abbildung, wie in der Vorlesung definiert. Zeigen Sie:

1. F^{-1} ist surjektiv,
2. $(F^{-1})^{-1} = F$,
3. F ist genau dann injektiv, wenn F^{-1} eine (eindeutige) Abbildung ist.

Abgabe: 10. Mai 2010

Aufgabe 1. (8 Punkte)

Wir wollen alle $n!$ Permutationen der Menge $A = \{0, 1, \ldots, n-1\}$ effektiv aufzählen, also eine explizite Bijektion zwischen S_A und der Menge $\{0, 1, \ldots, n! - 1\}$ herstellen.

a) Seien $a_1, \ldots, a_n \in \mathbb{N}, n \geq 1$. Setze $N_i := a_1 \cdots a_i$ für $1 \leq i \leq n$ und $N_0 := 1$. Man zeige, dass jedes $0 \leq x < N_n$ eine eindeutige Darstellung der Form

$$x = \sum_{i=0}^{n-1} x_i N_i \quad \text{mit } 0 \leq x_i < a_{i+1} \tag{1}$$

besitzt.

b) Man gebe eine Bijektion zwischen S_A und der Menge $\{0, 1, \ldots, n! - 1\}$ explizit an.

Hinweis: Wähle $a_i = i$ für $1 \leq i \leq n$ und stelle $0 \leq x < n!$ in der Form (1) dar. Konstruiere aus den Koeffizienten $x_0, \ldots, x_{n-1}$ eine Permutation.

In den restlichen Aufgaben sei $\mathcal{K}$ stets ein Kryptosystem mit allen zu Beginn von § 2.2 gemachten Annahmen. Die Aufgaben sind ohne Verwendung des Entropie-Begriffes zu bearbeiten.

Aufgabe 2. (8 Punkte)

Es sei $\mathcal{K}$ perfekt sicher und Φ frei.

a) Zeigen oder widerlegen Sie: μ_C ist für jede Verteilung μ_P gleichverteilt.

b) Zeigen Sie unter der Voraussetzung $|P| = |C|$: μ_C hängt nicht von μ_P ab.

c) (freiwillig) Lässt sich b) auch ohne die Voraussetzung $|P| = |C|$ zeigen?

Aufgabe 3. (8 Punkte)

Es sei Φ frei.

a) Angenommen es gibt eine Verteilung μ_P so, dass μ_C gleichverteilt ist. Warum folgt daraus nicht notwendigerweise, dass $\mathcal{K}$ perfekt sicher ist? Geben Sie ein Gegenbeispiel an.

b) Zeigen Sie: Wenn μ_C für jede Verteilung μ_P gleichverteilt ist, so ist $\mathcal{K}$ perfekt sicher.

Abgabe: 17. Mai 2010

Aufgabe 1. (8 Punkte)

In dieser Aufgabe sei $\mathcal{K}$ ein Kryptosystem mit allen zu Beginn von § 2.2 gemachten Annahmen. Ausserdem sei Φ frei.

a) Wir definieren zu jedem $c \in C$ die Menge $K(c) := \{e \in K \mid \exists p \in P : e(p) = c\}$ (die Menge aller Schlüssel, die zu c führen können). Sei μ_P beliebig. Zeigen Sie:

$\mathcal{K}$ ist genau dann perfekt sicher für μ_P, wenn μ_C auf jeder der Mengen $K(c)$ konstant ist.

b) Wir betrachten Verteilungen der Form $\mu_P(p_1) = \mu_P(p_2) = 1/2$ für $p_1 \neq p_2$ und $\mu_P(p) = 0$ für alle $p \neq p_{1,2}$, wie sie für die Untersuchung der Nicht-Unterscheidbarkeit (IND) relevant sind. Zeigen Sie:

$\mathcal{K}$ ist genau dann perfekt sicher, wenn $\mathcal{K}$ perfekt sicher für jedes μ_P dieser Form ist.

Aufgabe 2. (8 Punkte)

Es seien $X = \{x_1, \ldots, x_n\}, Y = \{y_1, \ldots, y_m\}$ zwei endliche Zufallsvariablen.

a) Zeigen Sie:

1. $H(X|Y) = -\sum_{i=1}^{n} \sum_{j=1}^{m} \mu_{X,Y}(x_i, y_j) \lg \mu_{X|Y}(x_i|y_j)$,
2. $H(X,Y) = H(X|Y) + H(Y)$,
3. $H(X|Y) \leq H(X)$.

b) Zeigen Sie, dass aus $H(X|Y) = 0$ folgt, dass $X = f(Y)$ für eine Funktion f.

c) Wir betrachten den unabhängigen Wurf zweier 6-seitiger Würfel. Auf dem dadurch gegebenen Wahrscheinlichkeitsraum (Ω, μ) mit $\Omega = \{1, \ldots, 6\}^2$ seien die Zufallsvariablen X, Y erklärt durch $X(w_1, w_2) = w_1 + w_2$ und $Y(w_1, w_2) = |w_1 - w_2|$. Bestimmen Sie $H(X), H(Y), H(X,Y)$, $H(X|Y)$ und $H(Y|X)$.

Aufgabe 3. (8 Punkte)

In dieser Aufgabe sei $\mathcal{K}$ ein Kryptosystem mit allen zu Beginn von § 2.4 gemachten Annahmen. Die Aufgabe ist unter Verwendung des Entropie-Begriffes zu bearbeiten. Es sei Φ frei.

a) Berechnen Sie zu dem Kryptosystem aus Beispiel 2.2.1 der Vorlesung bis auf zwei Nachkommastellen genau die Werte für $H(P), H(K), H(C), H(K|C), I(K,C), H(P|C), I(P,C)$. Angenommen, es werden wiederholt und unabhängig Klartexte gewählt und mit demselben Schlüssel verschlüsselt. Wie groß ist das Unizitätsmaß?

b) Zeigen Sie: Φ frei $\Leftrightarrow H_0(K) = 0$.

c) Zeigen Sie: $\mathcal{K}$ ist genau dann perfekt sicher, wenn $H(C)$ nicht von der Verteilung μ_P abhängt. *Hinweis: Die Verteilung μ_K ist fest; sie ist Teil des Kryptosystems $\mathcal{K}$.*

Abgabe: 31. Mai 2010

Aufgabe 1. (8 Punkte)

Es seien K ein Körper, $l \geq 1, c = (c_0, \ldots, c_{l-1}) \in K^l$ mit $c_0 \neq 0$. Zeigen Sie:

a) Für eine beliebige Folge $s = (s_n)$ in K mit $\operatorname{per} s < \infty$ gilt: s ist k-periodisch $\Leftrightarrow \operatorname{per} s | k$.

b) $\operatorname{per} c = \operatorname{kgV}\{\operatorname{per} \langle\, c, t \,\rangle \mid t \in K^l\}$.

c) Es gibt $t \in K^l$ mit $\operatorname{per} c = \operatorname{per} \langle\, c, t \,\rangle$.

d) Für jedes Polynom $f \in K[X]$ mit $f(0) \neq 0$ gilt: $f | X^k - 1 \Leftrightarrow \operatorname{ord} f | k$.

Aufgabe 2. (8 Punkte)

a) Gegeben sei das LFSR mit charakteristischem Polynom $\chi = X^5 + X + 1$ über $\mathbb{F}_2$. Bestimmen Sie alle Bahnen auf dem Raum $\mathbb{F}_2^5$ der Zustandsvektoren. Geben Sie zu jeder Bahn die Länge und einen Zustandsvektor als Repräsentanten an.

b) Bestimmen Sie die Ordnung des Polynoms $X^7 + X^4 + X^3 + X^2 + 1 \in \mathbb{F}_2[X]$.

c) Es sei $K = \mathbb{F}_2$ und $c \in K^l$ beliebig mit $c_0 \neq 0$. Ist χ_c irreduzibel, so ist $\operatorname{per} \langle\, c, t \,\rangle$ für $t \neq 0$ unabhängig von t (das folgt aus Korollar 3.2.6c) aus der Vorlesung). Zeigen oder widerlegen Sie die Umkehrung dieser Aussage.

Aufgabe 3. (8 Punkte)

Gegeben seien ein Modul $m \in \mathbb{N}$ sowie $a, b \in \mathbb{Z}_m$. Zu einem Startwert $t \in \mathbb{Z}_m$ wird eine Folge $s = (s_n)$ in $\mathbb{Z}_m$ mit $s_0 = t$ definiert durch die (inhomogene) lineare Rekursionsgleichung

$$s_{i+1} := a \cdot s_i + b, \quad i \geq 0.$$

Eine Vorschrift dieser Art zum Erzeugen von Folgen bezeichnet man als einen *Linearen Kongruenzgenerator*.

a) Zeigen Sie: Ist $(a, m) = 1$, so ist s periodisch. *Hinweis: Zu zeigen ist, dass keine Vorperiode existiert.*

Im Folgenden seien a, b fest gewählt mit $(a, m) = 1$. Es bezeichne r_t die kleinste Periodenlänge von s bei Startwert t. Offensichtlich ist $r_t \leq m$. Zeigen oder widerlegen Sie:

b) Gilt $r_t = m$ für einen Startwert t, so auch für alle Startwerte.

c) Ist $(b, m) \neq 1$, so ist $r_t < m$ für alle Startwerte t.

d) Sind b und m teilerfremd, so gilt $r_t = m$ für alle Startwerte t.

— bitte wenden —

Krypto-Challenge No. 3. (Autokey-Chiffre)

Als Alphabet A wird die Menge $\mathbb{Z}_{26}$ verwendet mit der Zuordnung `A`$= 0$, `B`$= 1$, usw. Zu einem Klartext $p = (p_1, p_2, \ldots, p_n) \in A^n$ wird ein one time-pad $e \in A^n$ erzeugt, wobei $e_1, \ldots, e_6$ zufällig gewählt sind und $e_i = p_{i-6}$ für $i > 6$. Der Geheimtext ist $c := p + e$ mit komponentenweiser Addition modulo 26.

Finden Sie zu dem auf der Webseite gegebenen Geheimtext die ersten 6 Schlüsselzeichen. Der Klartext ist in englischer Sprache und $n = 24000$.

Krypto-Challenge No. 4. (Feistel-Chiffre, known-plaintext)

Als Alphabet A wird die Menge $\mathbb{Z}_{26}$ verwendet mit der Zuordnung `A`$= 0$, `B`$= 1$, usw. Ein Klartext $p = (p_1, p_2, \ldots, p_n) \in A^n$ wird in 2er-Blöcke der Form $(a, b) = (p_i, p_{i+1})$ mit i gerade unterteilt. Diese 2-er Blöcke werden unabhängig voneinander verschlüsselt (wie unten beschrieben) und danach wieder aneinandergehängt, um den Geheimtext zu erhalten. Als Schlüssel ist eine feste Permutation $\pi \in S_A$ gewählt. Eine Verschlüsselungsrunde ist durch die Abbildung

$$(a, b) \mapsto (b, a + \pi(b))$$

gegeben, wobei die Addition modulo 26 gemeint ist. Davon werden zwei Runden angewendet (mit demselben "Rundenschlüssel" π).

Finden Sie zu dem auf der Webseite gegebenen Klar-/Geheimtextpaar den verwendeten Schlüssel π. Es ist $n = 64000$.

Abgabe: 7. Juni 2010

Aufgabe 1. (10 Punkte)

Es sei $K \subseteq L$ eine Körpererweiterung von endlichem Grad. Wir bezeichnen mit $\mathrm{Aut}_K(L)$ die Menge der Körperautomorphismen $\varphi : L \to L$, die K punktweise fixieren, d.h. $\varphi(x) = x$ für alle $x \in K$.

a) Zeige für alle $f \in K[X], \alpha \in L$: $f(\alpha) = 0 \Rightarrow f(\varphi(\alpha)) = 0$.
Hinweis: Zeige allgemeiner: $f(\varphi(\alpha)) = \varphi(f(\alpha))$.

Für die weiteren Aufgabenteile sei K endlich mit $q = p^r$ Elementen. Wir definieren:

$$\varphi : L \to L, \quad x \mapsto x^q$$

b) Zeige: $\varphi \in \mathrm{Aut}_K(L)$.

c) Zeige für alle $\alpha \in L$: $\mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\alpha^q, K)$.

d) Zeige: Für jeden irreduziblen Teiler f von $X^{q^m} - X \in K[X]$ ist $\deg f | m$.

e) Sei $f \in K[X]$ irreduzibel, $\deg f = n$. Zeige: Ist $\alpha \in L$ eine Nullstelle von f, so sind alle n paarweise verschiedenen Nullstellen von f gegeben durch: $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$.

Hinweis: Verwende c) und d).

Aufgabe 2. (8 Punkte)

Wir untersuchen den Körper $\mathbb{F}_{16}$. Das Polynom $f = X^4 + X + 1 \in \mathbb{F}_2[X]$ ist irreduzibel, also $\mathbb{F}_{16} \cong \mathbb{F}_2[X]/(f)$. Wir repräsentieren die Elemente von $\mathbb{F}_{16}$ durch ihren Koordinatenvektor, geschrieben als Zeilenvektor, bzgl. der $\mathbb{F}_2$-Basis $(1, X, X^2, X^3)$, also z.B. $\overline{1 + X^2}$ durch $(1, 0, 1, 0)$ oder kurz 1010. Setze $a := \overline{X} = 0100$. Wir wissen schon aus Beispiel 3.2.7, dass a primitives Element von $\mathbb{F}_{16}$ ist.

a) Listen Sie in einer Tabelle alle Potenzen von a sowie deren Darstellung als Zeilenvektoren auf. Bearbeiten Sie die folgenden Teilaufgaben anhand dieser Tabelle.

b) Berechnen Sie a^{-1} und a^{-7}.

c) Berechnen Sie die Bahnen des Automorphismus $\varphi : \mathbb{F}_{16} \to \mathbb{F}_{16}, x \mapsto x^2$ auf $\mathbb{F}_{16}$.

d) Welche Elemente machen den Teilkörper $\mathbb{F}_4$ aus?

e) Gruppieren Sie die Elemente mit gleichem Minimalpolynom über $\mathbb{F}_2$.
Hinweis: Aufgabe 1e).

f) Ordnen Sie die Minimalpolynome $X^4 + X^3 + X^2 + X + 1$ und $X^4 + X^3 + 1$ der richtigen Gruppe zu.

g) Gruppieren Sie die Elemente mit gleichem Minimalpolynom über $\mathbb{F}_4$.
Hinweis: Aufgabe 1e).

Aufgabe 3. (4 Punkte)

a) Es sei $L = \mathbb{F}_8$. Berechnen Sie zu jedem d die Anzahl der Elemente aus L vom Grad d über $\mathbb{F}_2$ (d.h. der $\alpha \in L$ für die $\deg \mathrm{Irr}(\alpha, \mathbb{F}_2) = d$ gilt), sowie die Anzahl der irreduziblen Polynome vom Grad d, die als Minimalpolynome von Elementen aus L über $\mathbb{F}_2$ auftreten.

b) Berechnen Sie die Anzahlen aus a) mit $L = \mathbb{F}_{64}$.

c) Berechnen Sie über $\mathbb{F}_2$ die Anzahl $A(d)$ für alle $1 \leq d \leq 11$, sowie für $d = 16$.

Abgabe: 14. Juni 2010

Aufgabe 1. (8 Punkte)

a) Zeigen Sie, dass in jeder endlichen abelschen Gruppe G gilt:

$$\max\{\operatorname{ord} g \mid g \in G\} = \operatorname{kgV}\{\operatorname{ord} g \mid g \in G\}.$$

Hinweis: Zeigen Sie dies möglichst elementar, insbesondere ohne Verwendung des Hauptsatzes über endliche abelschen Gruppen und ohne Sylow-Untergruppen zu betrachten.

b) Sei K ein beliebiger Körper. Folgern Sie aus a), dass jede endliche Untergruppe von K^* zyklisch ist.
Hinweis: Wählen Sie ein Element $a \in K^*$ maximaler Ordnung und betrachten Sie das Polynom $X^m - 1$ mit $m = \operatorname{ord} a$.

Aufgabe 2. (8 Punkte)

Diese Aufgabe baut auf Aufgabe 6/2 auf. *Hinweis: Wiederholt ist Aufgabe 6/1e) zu verwenden.*

a) Bestimmen Sie alle irreduziblen und alle primitiven quadratischen Polynome über $\mathbb{F}_4$.

b) Bestimmen Sie alle Linear-Rekursiven Folgen vom Grad 2 über $\mathbb{F}_4$ mit Periodenlänge 15.
Hinweis: Geben Sie zu jeder der vier Folgen jeweils eine vollständige Periode an.

Aufgabe 3. (8 Punkte)

a) Die *lineare Komplexität* einer Folge $s = (s_i)$ in K ist definiert als kleinstes $l \in \mathbb{N}$, für das $c, t \in K^l$ existieren mit $s = \langle c, t \rangle$. Berechnen Sie die lineare Komplexität sowie c und t für die Folgen

$$\begin{aligned} a &= 10101010101010, \\ b &= 001100110011, \\ c &= 1001000100001, \\ d &= 000000000001. \end{aligned}$$

b) Gegeben seien die Folgen

$$\begin{aligned} a &= 00100001111101010011000100001111101010011000100001, \\ b &= 00110000110110111001101001011010111101111011101111, \\ c &= 10011111000100001101010110011111000100001101010110 0. \end{aligned}$$

Davon wurde eine mittels LFSR, eine andere mit einem linearen Kongruenzgenerator aus Aufgabe 5/3, und die übrige zufällig erzeugt. Der lineare Kongruenzgenerator wurde mit Modul $m = 8$ betrieben und die Zahlen $0, \ldots, 7$ wurden in Binärdarstellung umgewandelt. Bestimmen Sie, welche Folge wie erzeugt wurde. Berechnen Sie dann für diejenige Folge, die mit einem linearen Kongruenzgenerator erzeugt wurde, die Parameter a und b.

Abgabe: 21. Juni 2010

Aufgabe 1. (4 Punkte)

Wie betrachten den Körper $F := \mathbb{F}_{2^8}$, dargestellt als $F = \mathbb{F}_2[X]/(f)$ mit dem AES-Polynom $f = X^8 + X^4 + X^3 + X + 1 \in F_2[X]$. Sei $a \in F$ eine Nullstelle von f.

Berechnen Sie möglichst effektiv die Ordnung von f.
Hinweis: f ist nicht primitiv.

Aufgabe 2. (8 Punkte)

Es seien F und a wie in Aufgabe 1 und weiter $h = X^4 + 1 \in F[X]$ und $R = F[X]/(h)$. Wir betrachten den Vektorraum F^4 und identifizieren den Vektor $(x_1, x_2, x_3, x_4)^T \in F^4$ mit dem Element $x_1X^3 + x_2X^2 + x_3X + x_4 \in R$. Es sei $c = (a+1, 1, 1, a)^T \in F^4$. Die Multiplikation in R definiert, unter der angegebenen Identifikation, eine lineare Abbildung $m : F^4 \to F^4, y \mapsto c \cdot y$.

a) Berechnen Sie die Matrix von m sowie alle Fixpunkte von m.

b) Begründen Sie kurz, warum die beiden AES-Abbildungen ShiftRows und MixColumns F-lineare Endomorphismen des Vektorraums F^{16} sind.
Hinweis: MixColumns ist definiert als die spaltenweise Anwendung von m auf $F^{4\times4}$, nachdem F^{16} mit $F^{4\times4}$ identifiziert wird.

c) Welche Dimensionen haben die Fixpunkträume von ShiftRows und MixColumns?

Abgabe: 28. Juni 2010

Aufgabe 1. (6 Punkte)

Es bezeichne p eine Primzahl, n eine natürliche Zahl, $\left(\frac{a}{p}\right)$ das Legendre-Symbol, $\left(\frac{a}{n}\right)$ das Jacobi-Symbol, und J_n die Menge $\{a \in \mathbb{Z}_n^* \mid \left(\frac{a}{n}\right) = 1\}$. Zeigen Sie:

a) Für $p > 2$ definiert das Legendre-Symbol $\left(\frac{\cdot}{p}\right)$ einen Gruppen-Epimorphismus von $\mathbb{Z}_p^*$ in die Gruppe $(\{\pm 1\}, \cdot)$.

b) Sei n ungerade und keine Quadratzahl. Dann ist J_n eine Untergruppe von $\mathbb{Z}_n^*$ mit Index $[\mathbb{Z}_n^* : J_n] = 2$.

c) Falls n Blum-Zahl ist, so gilt $[J_n : Q_n] = 2$ und $J_n = Q_n \cup -Q_n$.

Aufgabe 2. (7 Punkte)

Bestimmen Sie alle Blum-Zahlen ≤ 100. Bestimmen Sie anschliessend für die vier kleinsten Blum-Zahlen n jeweils:

1. die Mächtigkeiten von $Q_n, \widetilde{Q_n}$ und $\overline{Q_n}$,
2. alle Elemente von Q_n,
3. alle Bahnen der Rabin-Funktion auf Q_n,
   Hinweis: Mit Rabin-Funktion ist die Abbildung $Q_n \to Q_n, a \mapsto a^2$ gemeint.
4. alle möglichen Ausgabe-Sequenzen des Blum-Blum-Shub-Generators.

Aufgabe 3. (8 Punkte)

Machen Sie sich zunächst den probabilistischen Algorithmus zur Berechnung von Quadratwurzeln modulo p klar, der sich aus dem Beweis von Satz 4.3.13 ergibt.

a) Berechnen Sie damit eine Quadratwurzel von 5 modulo 19.

b) Berechnen Sie damit eine Quadratwurzel von 2 modulo 17.

c) Es sei bekannt, dass $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Warum kann mit dieser Information der Algorithmus für gewisse p deterministisch durchgeführt werden? Für welche p ist das der Fall?

Nun betrachten wir Quadratwurzeln modulo n, n keine Primzahl.

d) Sei $n = 713$. Berechnen Sie aus dem Hinweis $185^2 \equiv 1 \pmod{n}$ die Faktorisierung von n.
Hinweis: Vermuten Sie, es könnte sich bei n um eine Blum-Zahl handeln.

Abgabe: 5. Juli 2010

Aufgabe 1. (8 Punkte)

a) Es sei $e = 21$ ein öffentlicher Schlüssel für das Rabin-Kryptosystem. Geheimtexte $c \in \mathbb{Z}_n^*$ werden durch ihren kleinsten positiven Repräsentanten als Binärzahlen kodiert (das niedrigste bit steht rechts). Welcher der Texte 10000, 0001, 10101 ist als Geheimtext möglich? Berechnen Sie zu diesem alle möglichen Klartexte.

b) Es sei $n = 77$ ein öffentlicher Schlüssel für das Blum-Goldwasser-Kryptosystem. Wie in a) werden Elemente aus $\mathbb{Z}_n^*$ durch ihren kleinsten positiven Repräsentanten als Binärzahlen kodiert (das niedrigste bit steht rechts). Entschlüsseln Sie den Geheimtext 1000111111.
Hinweis: Das Blum-Goldwasser-Kryptosystem ergibt sich aus der Blum-Goldwasser-Konstruktion, wenn als Einweg-Permutation mit Hintertür die Rabin-Funktion verwendet wird.

Aufgabe 2. (6 Punkte)

a) Zeigen Sie, dass das Blum-Goldwasser Kryptosystem nicht das Sicherheitsmodell IND-CCA2 erfüllt. Beschreiben Sie dazu, wie ein Angreifer vorgeht, um das in Beispiel 1.3.15 beschriebene Spiel zu gewinnen.

b) Angenommen, SQROOT und QRP sind für Blum-Zahlen algorithmisch äquivalent, d.h. SQROOT reduziert sich polynomiell auf QRP. Erfüllt das Blum-Goldwasser Kryptosystem dann das Sicherheitsmodell TB-CCA2? Die Antwort ist zu begründen.

Aufgabe 3. (6 Punkte)

a) Vervollständigen Sie den Beweis von Satz 5.1.6 aus der Vorlesung um den letzten offenen Fall.
Hinweis: Zu zeigen ist folgende Aussage: Seien p, q verschiedene ungerade Primzahlen, und sei $t \in \mathbb{N}$ mit $\mathrm{ord}_{\mathbb{Z}_{p-1}}(t) = \mathrm{ord}_{\mathbb{Z}_{q-1}}(t) = 2^k$. Dann ist $\mathrm{ord}_{\mathbb{Z}_{p-1}}(xt) \neq \mathrm{ord}_{\mathbb{Z}_{q-1}}(yt)$ für die Hälfte aller Paare $(x, y) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_{q-1}$.

b) Es seien (n, e_1) und (n, e_2) zwei öffentliche RSA-Schlüssel, $x < n$ ein Klartext, und c_1, c_2 die zugehörigen Geheimtexte, d.h. $c_i = \Phi_{(n,e_i)}(x)$. Zeigen Sie unter der Voraussetzung, dass e_1, e_2 teilerfremd sind, wie x aus der Kenntnis von c_1, c_2 und den öffentlichen Schlüsseln berechnet werden kann.

Abgabe: 12. Juli 2010

Aufgabe 1. (8 Punkte)

Zeigen Sie:

a) Jede Carmichael-Zahl hat mindestens drei verschiedene Primfaktoren.
Hinweis: Lemma 6.2.3

b) n Carmichael-Zahl $\Leftrightarrow$ n zerlegbar, quadratfrei und $\forall p \in \mathbb{P}, p|n : (p-1)|(n-1)$.

c) Falls für ein $k \in \mathbb{N}$ sowohl $6k+1, 12k+1$ als auch $18k+1$ Primzahlen sind, so ist deren Produkt eine Carmichael-Zahl. (Man konstruiere das kleinste Beispiel.)

Aufgabe 2. (8 Punkte)

a) Es sei $n = 3^\alpha$ für ein $\alpha \in \mathbb{N}$. Wie in der Vorlesung bezeichne U_0 die Gruppe der Fermat-Nichtzeugen für die Zerlegbarkeit von n.

i) Bestimmen Sie U_0 und $|\mathbb{Z}_n^* : U_0|$ für den Fall $\alpha = 2$.

ii) Zeigen Sie $9|\operatorname{ord}_{\mathbb{Z}_n^*}(4)$ für den Fall $\alpha \geq 3$.

b) Es sei G eine abelsche Gruppe. Wir bezeichnen mit G_m den Kern der Abbildung $G \to G, x \mapsto x^m$. Zeigen Sie für alle $a \in G$: $(\operatorname{ord} a, m) = 1 \Rightarrow |G : G_m| \geq \operatorname{ord} a$.

c) Es sei $n \in \mathbb{N}$ ungerade, zerlegbar. Wie in der Vorlesung bezeichne N die Menge der Miller-Rabin-Nichtzeugen für die Zerlegbarkeit von n. Begründen Sie, dass sich Satz 6.3.5 unter der Voraussetzung $n \geq 11$ zu $|N| \leq \frac{\varphi(n)}{4}$ verbessern lässt.

Aufgabe 3. (7 Punkte)

a) Charakterisieren Sie die Menge aller $n \in \mathbb{N}$ für die gilt

i) es gibt $a, b, k \in \mathbb{Z}$ mit $a^2 - b^2 = kn$.

ii) es gibt $a, b \in \mathbb{Z}$ mit $a^2 - b^2 = n$.

Wir faktorisieren nun $n \in \mathbb{N}$ mit dem quadratischen Siebverfahren aus der Vorlesung.

b) Es sei $n = p \cdot q$ mit verschiedenen ungeraden Primfaktoren p, q. Setze $d := |p - q|$. Zeigen Sie, dass sich im Siebintervall mit der Breite $S = d/2$ stets ein a befindet, für das $a^2 - n$ ein Quadrat ist.

c) Es sei $n = 4417$. Vergleichen Sie die Breite der benötigten Siebintervalle bei Verwendung der Faktorbasen $\{-1, 2, 3, 7\}$ bzw. $\{-1, 2, 3, 13\}$.

Abgabe: 19. Juli 2010

Aufgabe 1. (7 Punkte)

Es bezeichne $\mathbb{P}^2(K)$ die projektive Ebene über dem Körper K und $\mathbb{F}_q$ den Körper mit q Elementen.

a) Bestimmen Sie alle Geraden von $\mathbb{P}^2(\mathbb{F}_2)$ und geben Sie diese als Punktmengen an. Skizzieren Sie die Geraden anschliessend in einem Graphen mit Knotenmenge $\mathbb{P}^2(\mathbb{F}_2)$.
Hinweis: Die Punkte sollen in projektiven Koordinaten geschrieben sein.

b) Leiten Sie eine Formel für die Anzahl der Punkte in $\mathbb{P}^2(\mathbb{F}_q)$ her.

c) Leiten Sie eine Formel für die Anzahl der Geraden in $\mathbb{P}^2(\mathbb{F}_q)$ her.

Aufgabe 2. (7 Punkte)

Es sei E eine Weierstraß-Gleichung der Form $y^2 = f(x)$ über einem Körper K.

a) Zeigen Sie für den Fall $\operatorname{char} K \neq 2$:

i) E singulär $\Leftrightarrow \operatorname{disc} f = 0$.
Hinweis: Die Diskriminante $\operatorname{disc} f$ *eines Polynoms* $f \in K[X]$ *ist definiert als* $\operatorname{disc} f := \prod_{i \neq j}(\alpha_i - \alpha_j)$, *wobei* $\alpha_1, \ldots, \alpha_n$ *die Nullstellen von* f *in einem Zerfällungskörper sind. Insbesondere gilt* $\operatorname{disc} f = 0$ *genau dann, wenn* f *eine mehrfache Nullstelle besitzt (im Zerfällungskörper).*

ii) E hat maximal eine Singularität.

b) Zeigen Sie für den Fall $K = \mathbb{F}_{2^n}, n \in \mathbb{N}$:

i) Jedes Element von K ist ein Quadrat.

ii) E ist singulär.

— bitte wenden —

Aufgabe 3. (8 Punkte)

Es sei $K = \mathbb{F}_{2^n}, n \in \mathbb{N}$.

a) Es sei $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ eine Weierstraß-Gleichung über K. Eine *lineare Transformation* der Variablen x, y ist eine Substitution von $\begin{pmatrix} x \\ y \end{pmatrix}$ durch $A\begin{pmatrix} x \\ y \end{pmatrix} + b$ mit $A \in \mathrm{GL}_2(K), b \in K^2$. Zeigen Sie:

i) Falls $a_1 \neq 0$, so kann E durch eine lineare Transformation auf eine Form mit $a_4 = 0$ gebracht werden, ohne a_1, a_3 zu verändern.

ii) Falls $a_1 = 0, a_3 \neq 0$, so kann E durch eine lineare Transformation auf eine Form mit $a_2 = 0$ gebracht werden, ohne a_1, a_3 zu verändern.

b) Geben Sie eine möglichst einfache Bedingung für die Singularität von E im Fall

i) $a_1 \neq 0, a_3 = 0$,

ii) $a_1 = 0, a_3 \neq 0$.

Hinweis: Sie dürfen die gemäß Teil a) vereinfachte Form von E voraussetzen.

c) Geben Sie alle elliptischen Kurven über $\mathbb{F}_2$ an.
Hinweis: Beschränken Sie sich in den beiden Fällen aus a) auf die entsprechende vereinfachte Form von E.

Aufgabe 4. (6 Zusatz- Punkte)

Es sei E eine elliptische Kurve über K. Wir betrachten die in der Vorlesung eingeführten Operationen $*$ und $+$ auf $E(\overline{K})$, $\overline{K}$ der algebraische Abschluß von K.

a) Zeigen Sie für alle $P, Q, R \in E(\overline{K})$:

i) $P * Q = R \Leftrightarrow Q * R = P$,

ii) $P + Q = O \Leftrightarrow P * Q = O$,

iii) $-P = P * O$.

b) Es sei $K = \mathbb{F}_5$ und $E : y^2 = x^3 + 2x - 1$. Berechnen Sie zu allen Elementen von $E(K)$ den diskreten Logarithmus zur Basis $P = (0, 2)$.

Abgabe: — (Besprechung am 21.7. in der Vorlesung)

Aufgabe 1. (ohne Punkte)

Zwei Teilnehmer A und B wollen über eine unsichere Verbindung einen geheimen Schlüssel austauschen, den sie danach zur Kommunikation mit einem symmetrischen Kryptosystem verwenden. Dazu benutzen sie das *Diffie-Hellman Protokoll*: A wählt eine Primzahl p, ein primitives Element g von $\mathbb{F}_p$, sowie ein $a \in \{0, \ldots, p-1\}$. A berechnet dann $x := g^a \in \mathbb{Z}_p^*$ und übermittelt an B die Daten (p, g, x). B wählt daraufhin ein $b \in \{0, \ldots, p-1\}$, berechnet $y := g^b \in \mathbb{Z}_p^*$ und übermittelt y an A. Der geheime Schlüssel ist $z = g^{ab}$, den offensichtlich beide aus den ihnen bekannten Daten berechnen können. Dieser wird anschliessend in einem symmetrischen Kryptosystem verwendet.

a) Ein passiver Angreifer hört die Kommunikation zwischen A und B mit. Welches Referenzproblem muss er lösen können, um den geheimen Schlüssel zu berechnen?

b) Ein aktiver Angreifer hat die Möglichkeit, die Kommunikation zwischen A und B mitzuverfolgen und beliebig zu verändern. Beschreiben Sie einen Angriff, der es ihm ermöglicht, sämtliche nachfolgende Kommunikation im Klartext mitzuverfolgen.

Aufgabe 2. (ohne Punkte)

Gibt es elliptische Kurven über $\mathbb{F}_p, p$ prim, die keine Punkte ausser O besitzen?
Gibt es elliptische Kurven über $\mathbb{F}_{p^n}, n > 1$, die keine Punkte ausser O besitzen?
Geben Sie ggf. Beispiele an.

Aufgabe 3. (ohne Punkte)

Lässt sich die Operation $*$ auf einer elliptischen Kurve E durch die Addition $+$ ausdrücken?

Aufgabe 4. (ohne Punkte)

Es sei $E : y^2 = f(x)$ eine elliptische Kurve über $\mathbb{R}$. Charakterisieren Sie auf geometrische Art anhand der Bilder aus der Vorlesung (siehe Webseite), was es bedeutet, dass ein Punkt $P \in E(\mathbb{R})$ die Ordnung $2, 3$ bzw. 4 hat.

Aufgabe 5. (ohne Punkte)

Es sei E eine elliptische Kurve über $\mathbb{F}_q$. Beschreiben Sie eine *Kodierungsfunktion*, die Klartexte aus $\{0,1\}^n$ in Punkte auf E übersetzt. Wie ist n zu wählen?
Hinweis: Denken Sie auch an die Möglichkeit probabilistischer Kodierung.

Klausur Modulprüfung Kryptographie, SS 2010

Lehrstuhl D für Mathematik, RWTH Aachen, Dr. Timo Hanke 26. Juli 2010

Dauer: 2h, Gesamtpunktzahl: 28 Punkte

Aufgabe 1. (8 Punkte)

a) Bestimmen Sie alle irreduziblen sowie alle primitiven Polynome vom Grad 2 über $\mathbb{F}_3$.

b) Bestimmen Sie alle linear rekursiven Folgen vom Grad 2 in $\mathbb{F}_3$, die Periodenlänge 8 besitzen.
Hinweis: Es reicht jeweils die Angabe einer vollen Periode mit einem beliebigen Startwert.

c) Wieviele irreduzible Polynome gibt es vom Grad 3 über $\mathbb{F}_3$?

d) Wie lautet die maximale Periodenlänge einer linear rekursiven Folge vom Grad 3 in $\mathbb{F}_3$? Wieviele verschiedene Perioden dieser Länge gibt es?

Aufgabe 2. (4 Punkte)

Es sei $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ mit $\alpha^4+\alpha+1 = 0$. Berechnen Sie mit dem Baby-Step-Giant-Step Algorithmus in der Gruppe $\mathbb{F}_{16}^*$ den diskreten Logarithmus zur Basis α folgender Elemente: $1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2$.

Aufgabe 3. (4 Punkte)

Es sei $\mathbb{F}_q$ ein Körper mit q ungerade.

a) Für welche q ist -1 ein Quadrat in $\mathbb{F}_q$?

b) Zeigen Sie, dass -1 genau dann ein Quadrat in $\mathbb{F}_q$ ist, wenn $\left(\frac{-1}{q}\right) = 1$ (Jacobi-Symbol).

Aufgabe 4. (6 Punkte)

Wir betrachten die Gleichung $E : y^2 = x^3 - x$ über dem endlichen Körper $K = \mathbb{F}_q$.

a) Für welche q definiert E eine elliptische Kurve über $\mathbb{F}_q$?

b) Es sei $q \equiv 3 \pmod 4$. Zeigen Sie, dass E zu jedem $x \in \mathbb{F}_q$ einen Punkt der Form (x, y) oder $(-x, y)$ besitzt.
Hinweis: Aufgabe 3.

c) Es sei $q \equiv 3 \pmod 4$. Wieviele Punkte besitzt E ?

d*) Es sei $q \equiv 3 \pmod 4$. Konstruieren Sie eine deterministische Kodierungsfunktion $\mathbb{F}_q \to E(\mathbb{F}_q)$, die sich auch effizient dekodieren lässt. (2 Bonus-Punkte)

— bitte wenden —

Aufgabe 5 stellt einen Auswahl-Teil dar: es ist entweder Aufgabe 5.1 oder 5.2 zu bearbeiten.

Aufgabe 5.1. (6 Punkte)

Es sei p eine Primzahl mit $p \equiv 5 \pmod 8$.

a) Leiten Sie eine explizite Formel für eine Quadratwurzel von -1 modulo p her.
Hinweis: Sie dürfen ohne Beweis verwenden, dass für jede Primzahl p gilt: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

b) Verwenden Sie die Formel aus a), um alle Quadratwurzeln von -1 modulo 29 zu berechnen.

c) Es sei $\left(\frac{a}{p}\right) = 1$. Leiten Sie eine explizite Formel für eine Quadratwurzel von a modulo p her.
Hinweis: Sie können sich an dem entsprechenden Algorithmus aus der Vorlesung/Übung orientieren. Verwenden Sie a). Die explizite Formel darf eine Fallunterscheidung enthalten.

d) Berechnen Sie mit der Formel aus c) eine Quadratwurzel von 3 modulo 13.

Aufgabe 5.2. (6 Punkte)

Es sei $n \in \mathbb{N}$ ungerade. Ein $a \in \mathbb{N}$ heißt *Solovay-Strassen-Zeuge* für die Zerlegbarkeit von n, falls $a^{n-1} \not\equiv 1 \pmod n$ oder $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod n$. Wir wollen zeigen, dass jedes ungerade, zerlegbare n einen Solovay-Strassen-Zeugen besitzt.

a) Zeigen Sie, dass man oBdA n von der Form

$$n = pm \text{ mit } p \text{ prim, } m \text{ ungerade, } p, m > 2 \text{ und } p \nmid m \tag{1}$$

annehmen kann. *Hinweis: Carmichael-Zahlen.*

b) Zeigen Sie, dass es für jedes n von der Form (1) ein a gibt mit $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod n$.
Hinweis: Wähle a mit $\left(\frac{a}{p}\right) = -1$ und $a \equiv 1 \pmod m$. Warum gibt es so ein a?

Aufgabe 6. (4 Bonus- Punkte)

Es seien $(n_1, e), \ldots, (n_r, e)$ öffentliche RSA-Schlüssel, und x ein Klartext mit $0 \le x < \min\{n_1, \ldots, n_r\}$. Weiter seien $c_i \equiv x^e \pmod{n_i}$ die zugehörigen Geheimtexte, $0 \le c_i < n_i$. Zeigen Sie unter der Voraussetzung, dass $r \ge e$ ist und $n_1, \ldots, n_r$ paarweise teilerfremd sind, wie x aus der Kenntnis von $c_1, \ldots, c_r$ und den öffentlichen Schlüsseln berechnet werden kann.
Hinweis: Betrachten Sie x als Element von $\mathbb{Z}$ und verwenden Sie den chinesischen Restsatz.

Beschreiben Sie kurz (in einem Satz), was diese Aussage für die praktische Verwendung von RSA bedeutet.

Viel Erfolg!