Übungen zur Kryptologie 1 Wintersemester 05/06
Johannes Köbler/Olaf Beyersdorff

Übungsblatt 11

Aufgabe 40 (mündlich)

Sei S eine Blockchiffre mit Blocklänge l und Schlüssellänge k. Wir betrachten einen Angriff bei *bekanntem Klartext*, d.h. es steht eine ausreichende Zahl von Klartext-Kryptotext-Paaren (x_i, y_i), $i = 1, \ldots, n$ zur Verfügung.

a) Bestimmen Sie grob die erwartete Anzahl von Schlüsseln K mit $S(K, x_i) = y_i$ für $i = 1, \ldots, n$. Wie lässt sich im Fall $n \geq k/l$ mittels $n2^k$ Verschlüsselungen der Schlüssel bestimmen?

b) Um die Sicherheit zu erhöhen wird nun das Kryptosystem $S \times S$ verwendet, d.h. es gibt nun 2^{2k} Schlüssel (K, K'). Zeigen Sie, wie sich im Fall $n \geq 2k/l$ mittels $n2^{k+1}$ Ver- und Entschlüsselungen der Schlüssel bestimmen lässt. Wie viel Speicherplatz benötigt Ihr Algorithmus?

c) Überlegen Sie sich, wie man den Platzbedarf in b) reduzieren kann, wenn man mehr Rechenzeit zur Verfügung stellt. Suchen Sie nach einer möglichst allgemeinen Beziehung für diesen so genannten Time-Memory-Tradeoff.

Aufgabe 41 (mündlich)

Der „normale“ Ablauf einer Entschlüsselung beim AES erfolgt nach folgendem Schema:

$\textsc{AddRoundKey}(K^{10})$
$\textsc{ShiftRows}^{-1}$
$\textsc{SubBytes}^{-1}$
`for i:= 9 downto 1 do`
  $\textsc{AddRoundKey}(K^i)$
  $\textsc{MixColumns}^{-1}$
  $\textsc{ShiftRows}^{-1}$
  $\textsc{SubBytes}^{-1}$
`end`
$\textsc{AddRoundKey}(K^0)$

Zeigen Sie, dass alternativ auch dieselbe Reihenfolge der Operationen wie bei der Verschlüsselung benutzt werden kann.

Aufgabe 42 (mündlich)

Berechnen Sie $\varphi(75\,600)$, $\varphi(14\,948)$, $\log_{7,3} 4$, $\log_{37,2} 3$, $\mathrm{ord}_7(2)$ und $\mathrm{ord}_{31}(2)$.

Aufgabe 43 (schriftlich, 10 Punkte)

a) Bestimmen Sie in $\mathbb{Z}_5[x]/3x^2 + 1$ den Repräsentanten für die Restklasse, in der das Polynom $2x^5 + x^4 + 4x + 3$ enthalten ist.

b) Bestimmen Sie alle irreduziblen Polynome $m(x)$ vom Grad 2 in $\mathbb{Z}_2[x]$. Stellen Sie jeweils die Additions- und Multiplikationstafeln für den Polynomrestklassenring $\mathbb{Z}_2[x]/m(x)$ auf.

c) Sei $m(x) = x^2 + 2$. Stellen Sie die Additions- und Multiplikationstafeln für den Polynomrestklassenring $\mathbb{Z}_3[x]/m(x)$ auf. Ist $\mathbb{Z}_3[x]/m(x)$ ein Körper?

d) Berechnen Sie das multiplikative Inverse von $g(x) = x^4 + x^2 + 2x$ in $\mathbb{Z}_3[x]/m(x)$, wobei $m(x) = 2x^6 + x^3 + x^2 + 2$ ist. Ist $m(x)$ irreduzibel über $\mathbb{Z}_3$?

Aufgabe 44 (mündlich)

a) Zeigen Sie, dass der Polynomrestklassenring $\mathbb{Z}_p[x]/m(x)$ genau dann ein Körper ist, wenn $m(x)$ irreduzibel über $\mathbb{Z}_p$ ist.

b) Zeigen Sie, dass zu jedem Polynom $f(x)$ in $\mathbb{Z}_p[x]$ ein endlicher Körper K existiert, der $\mathbb{Z}_p$ als Unterkörper enthält und in dem $f(x)$ in Linearfaktoren zerfällt (der kleinste solche Körper $K_p(f(x))$ ist bis auf Isomorphie eindeutig bestimmt und heißt der Zerfällungskörper für $f(x)$ über $\mathbb{Z}_p$).

c) Zeigen Sie, dass der Zerfällungskörper $K = K_p(x^{p^n} - x)$ genau p^n Elemente enthält. Schließen Sie hieraus auf die Existenz eines irreduziblen Polynoms $m(x)$ vom Grad n über $\mathbb{Z}_p$, indem Sie zu einem beliebigen Erzeuger g der multiplikativen Gruppe K^* von K ein Polynom $m(x)$ kleinsten Grades mit $m(g) = 0$ bestimmen.