Lehrstuhl für
Theoretische Informationstechnik

RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

Prof. Dr. R. Mathar

Kryptographie I,II

Zusatzübung

12. Juli 2007

Aufgabe 1. (13 Punkte)
Gegeben sei ein Kryptosystem mit Klartextraum und Schlüsseltextraum $\mathcal{M} = \mathcal{C} = \{0,1\}^4$.
Die Schlüssel sind Paare (A, B) von *regulären* Matrizen der Form

$$A = \begin{pmatrix} 1 & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathbb{F}_2^{2\times 2}, \qquad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & 1 \end{pmatrix} \in \mathbb{F}_2^{2\times 2}.$$

Die Verschlüsselung ist gegeben durch

$$e : \mathcal{M} \times \mathcal{K} \to \mathcal{C} : (m_1, m_2, m_3, m_4) \mapsto (c_1, c_2, c_3, c_4)$$

mit $\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = A \begin{pmatrix} m_1 \\ m_2 \end{pmatrix}$ und $\begin{pmatrix} c_3 \\ c_4 \end{pmatrix} = B \begin{pmatrix} m_3 \\ m_4 \end{pmatrix}$.

a) Bestimmen Sie die Kardinalität $|\mathcal{K}|$ des Schlüsselraumes.

b) Ist dieses System perfekt sicher, wenn der Schlüssel gemäß einer Gleichverteilung gewählt wird? Begründen sie Ihre Antwort.

c) Dieses Kryptosystem lässt sich auch als Blockchiffre auf Texte beliebiger Länge anwenden, hierbei beträgt die Blocklänge 4.
Verschlüsseln Sie den Klartext 0010 1011 1110 0110 mit dieser Blockchiffre im CBC-Modus mit Initialvektor $C_0 = (1, 0, 0, 1)$ und Schlüssel

$$K = (A, B) = \left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right).$$

Aufgabe 2. (13 Punkte)
Sei p eine Primzahl. Betrachten Sie die Menge

$$G := \{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_p \} \subseteq \mathbb{F}_p^{2\times 2}.$$

a) Zeigen Sie, dass die Menge G eine zyklische Gruppe bzgl. Matrixmultiplikation ist. Geben Sie einen Erzeuger an und bestimmen Sie die Gruppenordnung.

b) Formulieren Sie den DH-Schlüsselaustausch für G.

c) Warum ist dieses Protokoll unsicher?

Aufgabe 3. (14 Punkte)

a) Beweisen Sie die folgende Aussage:
Es seien $n \in \mathbb{Z}$ ungerade und $a \in \mathbb{Z}_n^*$. Wenn $a^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}$, dann ist n zusammengesetzt.

b) Formulieren Sie einen probabilistischen Primzahltest, der auf der Aussage aus Aufgabenteil a) basiert.

c) Beantworten Sie folgende Fragen zu dem Test aus Aufgabenteil b):

- Antwortet der Test immer korrekt, wenn n prim ist?
- Ist n zusammengesetzt, wenn der Test „n zusammengesetzt“ ausgibt?

Aufgabe 4. (10 Punkte)
Sie haben den Schlüsseltext $c = 1395$ abgefangen, der mit dem RSA-Verfahren verschlüsselt wurde. Da Sie wissen, an wen die Nachricht gesendet wurde, finden Sie den zugehörigen öffentlichen Schlüssel $(n, e) = (2419, 1617)$. Wie lauten die Nachricht und der private Schlüssel?

Aufgabe 5. (13 Punkte)
Gegeben sei der ElGamal-Public-Key $(p, a, y) = (107, 2, 61)$.

a) Zeigen Sie, dass dieser Schlüssel ein gültiger ElGamal-Public-Key ist.

b) Berechnen Sie den zugehörigen privaten Schlüssel.

c) Gegeben sei eine Nachricht m mit Hashwert $h(m) = 42$. Bestimmen Sie eine gültige ElGamal-Signatur (r, s) für diese Nachricht mit dem in Aufgabenteil b) berechneten privaten Schlüssel. Wählen Sie dabei im ersten Schritt $k = 17$.

Aufgabe 6. (14 Punkte)
Es sei G eine endliche, multiplikative, kommutative Gruppe und seien $a \neq b$ Erzeuger von G. Eine Funktion $h : \{0,1\}^* \to G$ sei gegeben durch den folgenden Algorithmus:

Input: Eine Nachricht m in Binärdarstellung $(m_1, m_2, \ldots, m_n)$
Output: Ein Gruppenelement $h(m) = r \in G$

```
r ← a
for (i ← 1; i ≤ n; i++) do
    if (m_i = 1) then
        r ← r · a
    else
        r ← r · b
    end if
end for
return r = h(m)
```

a) Geben sie eine geschlossene Form des von dem Algorithmus berechneten Funktionswertes $h(m)$ an.

b) Die Funktion h wird nun als Hashfunktion verwendet. Wie kann eine Kollision zu einer Nachricht m mit $m \neq 0$ und $m \neq 2^n - 1, n \in \mathbb{N}$, erzeugt werden, wenn weder die Gruppenordnung von G, noch die diskreten Logarithmen $\log_a b$ und $\log_b a$ bekannt sind?

c) Auf welche andere Weise kann eine Kollision zu einer gegebenen Nachricht m der Länge $|m| \geq 1$ erzeugt werden, wenn $\log_a b$ und $\log_b a$ bekannt sind?

d) Auf welche andere Weise kann eine Kollision zu einer gegebenen Nachricht m erzeugt werden, wenn die Gruppenordnung von G bekannt ist?

Anmerkung: Eine Gruppe G heißt kommutativ, wenn für alle $a, b \in G$ gilt, dass $a \cdot b = b \cdot a$.

Aufgabe 7. (10 Punkte)

Kreuzen Sie für die folgenden Aussagen jeweils an, ob sie wahr oder falsch sind.

Für jede richtige Antwort gibt es einen Punkt, für jede falsche Antwort wird ein Punkt abgezogen. Für nicht beantwortete Fragen erhält man keine Punkte. Die minimale Gesamtpunktzahl für diese Aufgabe ist 0.

Aussage	**wahr**	**falsch**
Es gilt für jedes Kryptosystem $H(\hat{C}) = H(\hat{M}) - H(\hat{K} \mid \hat{C})$.	☐	☐
Den Friedmanntest verwendet man zur Bestimmung der Schlüsselwortlänge einer Vigenère-Verschlüsselung.	☐	☐
Für ein perfekt sicheres Kryptosystem gilt $\lvert\mathcal{K}_+\rvert \geq \lvert\mathcal{C}_+\rvert$.	☐	☐
Sei X eine endlich diskrete Zufallsvariable mit Träger $\{x_1, \ldots, x_m\}$. Dann gilt für die Entropie $H(X)$, dass $0 \leq H(X) \leq \log m$.	☐	☐
Ein englischer Text wird mit einer Vigenère-Verschlüsselung mit Stromschlüssel verschlüsselt. Der Schlüssel entstammt ebenfalls der englischen Sprache. Die Wahrscheinlichkeit dafür, dass ein zufällig herausgegriffener Buchstabe des Kryptogramms in der Menge der häufigsten sieben Buchstaben $\{E, T, A, O, I, N, S\}$ liegt, ist ungefähr $0,57^2 = 0,3249$.	☐	☐
Jede stark kollisionsresistente Hash-Funktion ist schwach kollisionsresistent.	☐	☐
Seien $p \neq q$ prim und sei $n = p \cdot q$. Dann hat die Gleichung $x^2 \equiv 1 \pmod{n}$ immer 4 verschiedene Lösungen.	☐	☐
Die Expansionsabbildung E im DES-Algorithmus ist von der Form $E : \{0,1\}^{32} \to \{0,1\}^{48}$.	☐	☐
Die Blocklänge der AES-Verschlüsselung beträgt immer 128 Bit.	☐	☐
Seien $p \neq q$ prim und sei $n = p \cdot q$. Findet man eine Lösung der Gleichung $x^2 \equiv 1 \pmod{n}$, so kann man n faktorisieren.	☐	☐

Aufgabe 8. (13 Punkte)
Gegeben sei die Weierstrass-Gleichung

$$y^2 = x^3 + 1$$

über dem Körper $\mathbb{F}_7$.

a) Zeigen Sie, dass diese Gleichung eine elliptische Kurve E definiert.

b) Wie viele Elemente enthält die Menge $E(\mathbb{F}_7)$?

c) Betrachten Sie nun die Menge $E(\mathbb{F}_{7^4})$. Geben Sie sinnvolle obere und untere Schranken für die Kardinalität dieser Menge an.

d) Bestimmen Sie das Inverse der Punkte $(2, 3)$ und $(5, 0)$ in der Gruppe $E(\mathbb{F}_7)$.