Probeklausur SS09

Aufgabe 1. (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**
Jede affine Chiffre ist eine Hill-Chiffre.	☐	☐
Für den Erwartungswert des Koinzidenzindexs gilt: $E(I_C) = \sum_{l=1}^{m} q_l{}^2$, wobei die Einträge des Kryptogramms $\mathbf{C} = (C_1, \ldots, C_n)$ stochastisch unabhängig, identisch verteilt sind mit $P(C_i = l) = q_l$, $i = 1, \ldots, n$, $l = 1, \ldots, m$.	☐	☐
Für stochastisch unabhängige, identisch verteilte Zufallsvariablen X, Y gilt: $H(X,Y) = 2\,H(X)$.	☐	☐
Die Vernam-Chiffre ist perfekt sicher.	☐	☐
Die Funktion SubBytes des AES-Algorithmus ist linear.	☐	☐
Für alle Eingaben $n \in \mathbb{N}$ liefert der Primzahltest von Fermat (FPT): $P(\text{FPT states „n composite“} \mid \text{n composite}) > 0$.	☐	☐
4 ist eine Primitivwurzel modulo 63.	☐	☐
Für jedes $a \in \mathbb{Z}_p \backslash \{0\}$, p prim, existiert das multiplikative Inverse modulo p.	☐	☐
Die Sicherheit im ElGamal-Kryptosystem beruht auf dem Faktorisierungsproblem.	☐	☐
In der zyklischen Gruppe $\mathbb{F}_{2^4}^*$, deren Elemente Polynome vom Grad kleiner 4 über $\mathbb{F}_2$ sind und deren Multiplikation modulo $f(u) = u^4 + u + 1$ berechnet wird, mit irreduziblen Generator $a = (0010)$ gilt $a^{16} = 1$.	☐	☐

Aufgabe 2: (11 Punkte)

Sie hören ein Selbstgespräch eines Studenten, der für seine Klausur lernt. Dabei erfahren Sie, dass er eine Nachricht mit einer Vigenère-Chiffre verschlüsselt. Der **englische** Klartext beginnt mit „well“ und die Schlüssellänge ist 6. Sie fangen dazu den folgenden verschlüsselten Text ab.

ymasxygmmlvtkatuyddmgaafkahvpmgl

(a) Bestimmen Sie den Schlüssel und die Nachricht.

Anschließend beschäftigt sich der Student mit affinen Chiffren mit Schlüssel (a, b), $a, b \in \mathbb{Z}_{26}$. Sie hören, dass er den Buchstaben Z jeweils zu den drei Alphabeten $\Sigma_1 = \{A, \ldots, Z\}$, $\Sigma_2 = \{A, \ldots, Z, ,, ., \sqcup\}$ und $\Sigma_3 = \{0, \ldots, 9, \sqcup, A, \ldots, Z\}$, die mit den Mengen $\mathbb{Z}_{26}$, $\mathbb{Z}_{29}$ und $\mathbb{Z}_{37}$ identifiziert werden, verschlüsselt. Als Ergebnis erhält er 12, 22 bzw. 23.

(b) Bestimmen Sie den verwendeten Schlüssel.

Aufgabe 3. (16 Punkte)

Betrachten Sie das folgende Kryptosystem mit Nachrichtenraum $\mathcal{M}$ und Kryptogrammraum $\mathcal{C}$ mit $\mathcal{M} = \mathcal{C} = \{0,1\}^6$. Eine Nachricht $\mathbf{m} = (m_1, m_2, m_3, m_4, m_5, m_6)$ wird mit Hilfe der invertierbaren Matrizen

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 1 & e \\ f & g \end{pmatrix} \in \mathbb{F}_2^{2\times 2}$$

in Abhängigkeit von $k \in \mathbb{Z}_2$ wie folgt verschlüsselt.

$$e(m_1, m_2, m_3, m_4, m_5, m_6) = (c_1, c_2, c_3, c_4, c_5, c_6)$$

mit

$$\begin{aligned} (c_1, c_2)' &= \mathbf{A}(m_1, m_3)', \\ (c_3, c_4)' &= \mathbf{B}(m_5, m_6)', \\ (c_5, c_6) &= \begin{cases} (m_2, m_4) & \text{falls } k = 0, \\ (m_4, m_2) & \text{sonst.} \end{cases} \end{aligned}$$

(a) Charakterisieren Sie den Schlüsselraum und bestimmen Sie seine Mächtigkeit.

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

Betrachten Sie nun $k = 0$ und

$$\mathbf{A} = \mathbf{B} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

(c) Geben Sie eine Entschlüsselungsvorschrift $\mathbf{m} = d(\mathbf{c})$ für ein Kryptogramm $\mathbf{c} = (c_1, c_2, c_3, c_4, c_5, c_6)$ an. Entschlüsseln Sie damit das Kryptogramm $\mathbf{c} = (0, 1, 1, 1, 0, 0)$.

Das obige System kann als Blockchiffre auf Texte beliebiger Länge angewendet werden.

(d) Verschlüsseln Sie den Text $\mathbf{m} = (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$ im Output Feedback Mode (OFB) mit $C_0 = (0, 0, 1, 1, 0, 0)$.

(e) Wie lautet die Verschlüsselung des gleichen Textes bei gleichem C_0 im Cipher Feedback Mode (CFB)?

Aufgabe 4: (13 Punkte)

Betrachtet wird das Diffie-Hellman-Schlüsselaustauschprotokoll (DHP) mit Parametern p und a.

(a) Erklären Sie die Parameter und den Ablauf des DHPs.

(b) Zeigen Sie mit Hilfe des Fermat-Primzahltests, dass $p = 2^{15} + 5$ keine Primzahl ist.

(c) Benutzen Sie die Primzahl $p = 32843$ als Parameter. Sind die Wahlen $a_1 = 2$ und $a_2 = 32842$ als Parameter für das DHP geeignet?

Hinweise:

- 16421 ist eine Primzahl.
- Es gilt $2^{(2^{14})} = 2^{16384} \equiv 8243 \mod p$.

(d) Nun führen Alice und Bob mit geeigneten Parametern aus (c) und den geheimen Schlüsseln $x_A = 148$ und $x_B = 222$ das DHP durch. Bestimmen Sie den gemeinsamen Schlüssel.

Aufgabe 5: (12 Punkte)
Betrachtet wird das RSA Kryptosystem.

(a) Wie viele RSA-Schlüssel existieren für gegebene Primzahlen p und q?

Mit dem Miller-Rabin Primzahltest lassen sich große Primzahlen für die Verwendung in RSA finden.

(b) Beschreiben Sie den Test und bestimmen Sie eine obere Schranke für die Wahrscheinlichkeit, dass die gefundene Zahl tatsächlich prim ist, wenn der Test n mal unabhängig angewendet wird.

Alice sendet den Chiffretext $c = 3$ an Bob. Außerdem konnte Eve erfahren, dass $\varphi(n) = 4096$ und Bobs öffentlicher Schlüssel $e = 241$ ist.

(c) Entschlüsseln Sie die von Alice an Bob gesendete Nachricht.

Aufgabe 6. (11 Punkte)
Die erste Eigenschaft einer kryptografischen Hashfunktion ist, dass sie einfach zu berechnen sein soll.

(a) Wie lauten die weiteren drei Eigenschaften?

Nun soll mit einer sicheren, schnellen Blockchiffre $C_K(M)$ (z.B. AES) eine Hashfunktion erzeugt werden. Die Blockchiffre besitzt die Block- und Schlüssellänge n.

(b) Erzeugen Sie mit Hilfe der Blockchiffre eine Funktion f, die alle Bedingungen aus (a) erfüllt und Eingangsnachrichten der Länge n auf Ausgabenachrichten der Länge n abbildet.

Die folgenden drei Konstruktionsschemata werden vorgeschlagen, um die Funktion f aus (b) zu einer allgemein verwendbaren Hashfunktion zu erweitern. Die Eingangsnachricht $M = (m_1 m_2 m_3 \dots m_k)$ besteht aus Blöcken $m_1, \dots, m_k$ der Länge n.

1. $h^{(1)}(M)$:
   $h_0 \leftarrow 0$
   for $i \leftarrow \{1, \dots, m\}$:
   $h_i \leftarrow f(h_{i-1} \bigoplus m_i)$
   return h_m

2. $h^{(2)}(M)$:

   $h_0 \leftarrow 0$
   for $i \leftarrow \{1, \ldots, m\}$:
   $h_i \leftarrow h_{i-1} \bigoplus f(m_i)$
   return h_m

3. $h^{(3)}(M)$:

   $t_0 \leftarrow 0$
   for $i \leftarrow \{1, \ldots, m\}$:
   $t_i \leftarrow t_{i-1} \bigoplus m_i$
   $h_i \leftarrow f(t_i)$
   return h_m

(c) Finden Sie für die drei vorgestellten Schemata Nachrichten, die mindestens eine der Eigenschaften aus (a) verletzen und benennen Sie das verletzte Kriterium.

Aufgabe 7: (12 Punkte)
Alice hat zwei Dokumente m_1 und m_2 mit dem ElGamal-Signaturverfahren digital signiert. Die beiden Signaturen sind

$$(r_1, s_1) = (641, 1946) \text{ und } (r_2, s_2) = (641, 415).$$

Der öffentliche Schlüssel von Alice ist $(p, a, y) = (4663, 2, 3004)$. Die Dokumente wurden mit der Hashfunktion h vor dem Signieren auf $h(m_1) = 4012$ und $h(m_2) = 1985$ abgebildet. Was hat Alice falsch gemacht? Brechen Sie das Kryptosystem, indem Sie den privaten Schlüssel x von Alice bestimmen.

Aufgabe 8: (15 Punkte)
Gegeben sei die folgende Kurvengleichung

$$E_a : y^2 = x^3 + a.$$

Die Kurve sei definiert über $\mathbb{F}_{11}$, d.h. $a \in \mathbb{F}_{11}$.

(a) Für welche Werte von a beschreibt E_a eine elliptische Kurve über $\mathbb{F}_{11}$?

Nun sei $a = 4$.

(b) Geben Sie alle Punkte an. Wie viele Punkte hat $E_4(\mathbb{F}_{11})$?

(c) Bestimmen Sie zu jedem Punkt $P \in E_4(\mathbb{F}_{11})$ sein Inverses $-P$.

Nun werde die Kurve E_7 mit den Punkten $P_1 = (4, 4)$ und $P_2 = (4, 7)$ betrachtet.

(d) Bestimmen Sie $2P_1$ und $P_1 + P_2$ in $E_7(\mathbb{F}_{11})$.