Übung 2

Abgabe: 25.10.2018 **bis** 12:15 Uhr

1. Modulare Arithmetik I 10 Punkte

Berechnen Sie jeweils ohne Taschenrechner. Beschreiben Sie kurz den Zusammenhang zwischen den einzelnen Aufgaben.

a) $7 \cdot 5 \bmod 19$

b) $7 \cdot 81 \bmod 19$

c) $26 \cdot 43 \bmod 19$

d) $-12 \cdot 43 \bmod 19$

Hinweis: Die Ergebnisse sollten im Bereich $0, 1, \ldots,$ (Modulus - 1) liegen.

2. Modulare Arithmetik II 10 Punkte

Versuchen Sie bei jeder Aufgabe die Berechnungen auf verschiedene Arten durchzuführen, d. h. wenden Sie die Moduloreduktion einmal nur am Ende und das andere Mal auf alle Zwischenergebnisse an. Das Endergebniss sollte jeweils im Bereich $0, 1, \ldots,$ (Modulus - 1) liegen.

a) $(2 \cdot 5) \cdot 10 \bmod 13$

b) $2^3 \cdot 8 \bmod 250$

c) $7 \cdot 11 \bmod 11$

d) $3 \cdot 8 - 11 \cdot 6 \bmod 250$

e) $(2 \cdot 5 - 19) \cdot 5^6 \bmod 75$

f) $\frac{74}{7} \bmod 11$

g) $\frac{5 \cdot 2 - 8}{7^2} \bmod 11$

3. Modulare Arithmetik III 10 Punkte

Berechnen Sie jeweils ohne Taschenrechner. Bestimmen Sie die multiplikative Inverse durch **Ausprobieren**.

a) $5^{-1} \bmod 13$

b) $3 \cdot 4 \cdot 4^{-1} \bmod 13$

c) $3 \cdot 2 \cdot 4^{-1} \bmod 13$

d) $3 * x \equiv 3 \bmod 9$ (Geben Sie hier **alle** Lösungen an!)

4. Multiplikative Inverse 10 Punkte

a) Welche Elemente in $\mathbb{Z}_{13}, \mathbb{Z}_{14}$ und $\mathbb{Z}_{16}$ haben keine multiplikative Inverse?

b) Wie unterscheidet sich der Ring $\mathbb{Z}_{11}$ von $\mathbb{Z}_9$ und $\mathbb{Z}_{15}$ in Bezug auf die Elemente und deren multiplikative Inverse?

5. Mehrfache Verschlüsselung 15 Punkte

Eine beliebte Methode, um die Sicherheit von symmetrischen Algorithmen zu erhöhen, beruht auf der Idee, denselben Algorithmus mehrfach anzuwenden:

$$y \equiv e_{k_2}(e_{k_1}(x)) \bmod n$$

Wie oft in der Kryptologie sind die Dinge sehr knifflig und das reale Ergebnis weicht vom gewünschten Ergebnis ab. In dieser Aufgabe werden wir zeigen, dass die Doppelverschlüsselung von affinen Chiffren nicht sicherer ist als die einfache Verschlüsselung!
Angenommen wir haben zwei affine Chiffren $e_{k_1}(x) = y \equiv a_1 x + b_1 \bmod n$ und $e_{k_2}(x) = y \equiv a_2 x + b_2 \bmod n$.

a) Zeigen Sie, dass es eine affine Chiffre $e_{k_3}(x) \equiv a_3 x + b_3 \bmod n$ gibt, die genau dieselbe Verschlüsselung (und Entschlüsselung) wie die Kombination $e_{k_2}(e_{k_1}(x))$ erzeugt.
(5 Pkt.)

b) Bestimmen Sie a_3 und b_3 mit $a_1 = 7, b_1 = 13$ und $a_2 = 19, b_2 = 7$ und dem Modulus $n = 26$
(5 Pkt.)

c) Beschreiben Sie kurz was passiert, wenn Sie eine Brute-Force Attacke gegen die Zweifachverschlüsselung der affinen Chiffre anwenden. Hat sich der effektive Schlüsselraum vergrößert? Kennen Sie einen effektiveren Angriff auf die affine Chiffre, als einen Brute-Force-Angriff?
(5 Pkt.)

Bemerkung: Die Verwendung von Mehrfachverschlüsselung ist von großer praktischer Bedeutung. Bei DES erhöht sich z.B. die Sicherheit, wenn wir diesen dreimal hintereinander anwenden – wir werden dieses Thema in ein paar Wochen in der Vorlesung behandeln.

6. Cäsar-Chiffre 20 Punkte

Ein alternatives Verfahren zur Substitionschiffre ist die Cäsar-Chiffre, auch bekannt als Verschiebechiffre. Hier wird anstatt einer beliebigen Zuordnung für jeden Buchstaben (z.B. $A \mapsto T, B \mapsto X, C \mapsto F, \ldots$) lediglich eine Verschiebung des gesamten Alphabets um einen geheimen Offset (Verschiebungswert) vorgenommen.
So wird bspw. für den Offset $k = 5$ eine Verschiebung des Alphabets um 5 Zeichen durchgeführt ($A \mapsto F, B \mapsto G, C \mapsto H, \ldots$), und mit dieser Abbildung der Klartext kodiert.

a) Entschlüsseln Sie das Wort `MujmllmlAmkczqbg` mit der Cäsar-Chiffre und dem geheimen Offset $k = 8$. (5 Pkt.)

b) Vergleichen Sie die Sicherheit der Cäsar- und der Substitutions-Chiffre bezüglich statistischer Angriffe. Ist die Cäsar-Chiffre sicherer? (5 Pkt.)

c) Wenn Sie den Offset für jedes Klartextzeichen von einem beliebigen Startpunkt an inkrementieren (jeweils um eins erhöhen), wird dadurch die Sicherheit des Verfahrens gegen statistische Angriffe erhöht? (10 Pkt.)
Hinweis: Zum besseren Verständnis des Verfahrens sei folgendes Beispiel gegeben:

```
Klartext:   i n t e r n e t
Offset:     1 2 3 4 5 6 7 8
Geheimtext: J P W I W T L B
```

7. Reading Assignment 24 Punkte

Lesen Sie den Artikel *"Why cryptography is harder than it looks"* von Bruce Schneier. Der Inhalt dieses Textes ist prüfungsrelevant. Beantworten Sie die folgenden Fragen in jeweils 1-2 Sätzen:

a) Wie lange gilt ein System als sicher?

b) Was bringt dem Angreifer im Vergleich zum Verteidiger einen immensen Vorteil ein?

c) Was muss außer der reinen Mathematik alles berücksichtigt werden, damit ein System sicher ist?

d) Worin liegt der Unterschied in der Analyse eines Flugzeugunglücks und eines erfolgreichen Angriffs auf ein kryptographisches System?

e) Warum ist die Marketing-Politik bei entdeckten Sicherheitslücken in kryptographischen Anwendungen nicht detailliert über diese zu informieren problematisch?

f) Warum reicht es nicht ein sicheres kryptographisches System zu entwickeln? Was muss noch berücksichtigt werden damit Dieses System Daten und Resourcen schützen kann?