Aufgaben

1.1. Das nachfolgende Chiffrat in englischer Sprache wurde mit der Substitutionschiffre verschlüsselt. Das Ziel ist es, den Klartext zu erhalten.

```
  lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi
bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx
ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr
yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk
lmird jk xjubt trmui jx ibndt

  wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi
iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m
vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd
wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr
jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii
ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh
mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb
bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd
wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr
riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb
```

1. Berechnen Sie die Häufigkeit aller Buchstaben `A...Z` im Chiffrat. Dies kann von Hand mit Papier und Bleistift erfolgen oder mit Computerunterstützung, beispielsweise mit dem Programm CrypTool [4].
2. Entschlüsseln Sie das Chiffrat mittels Frequenzanalyse unter Benutzung einer Häufigkeitstabelle für die englische Sprache. Man beachte, dass der Text relativ kurz ist und die hier auftretenden Häufigkeiten von denen in Tabellen leicht abweichen können.
3. Wer schrieb den Text?

1.2. Der folgende Geheimtext wurde mit der Verschiebechiffre erzeugt:

```
  xultpaajcxitltlxaarpjhtiwtgxktghidhipxciwtvgtpilpit
ghlxiwiwtxgqadds.
```

1. Brechen Sie die Chiffre mittels Frequenzanalyse. Die Verschlüsselung von wie vielen Buchstaben muss mit der Frequenzanalyse erkannt werden, um den Schlüssel zu berechnen? Wie lautet der Klartext?
2. Wer ist der Autor?

1.3. In dieser Aufgabe wird die Langzeitsicherheit von AES mit 128-Bit-Schlüsseln betrachtet. Die Annahme ist, dass der beste bekannte Angriff die vollständige Schlüsselsuche ist. (AES ist die momentan am häufigsten eingesetzte symmetrische Chiffre.)

1. Wir nehmen an, dass der Angreifer spezielle Hardware-ICs, sogenannte ASICs, hat, die für AES-Schlüsseltests optimiert sind. Ein ASIC kann $5 \cdot 10^8$ Schlüssel pro Sekunde überprüfen und der Angreifer verfügt über ein Budget von einer Million Euro. Ein einzelnes ASIC kostet 50 € und es wird ein Overhead von 100 % für die Integration der ASICs angenommen (Bau des Computers, Stromversorgung, Kühlung usw.).
   Wie viele ASICs kann man mit dem gegebenen Budget parallel betreiben? Wie lange dauert eine vollständige Schlüsselsuche im Durchschnitt? Setzen Sie diese Zeit in Relation zu dem Alter des Universums, welches 10^{10} Jahre beträgt.
2. Wir schätzen nun die Entwicklung der Rechenleistung zukünftiger Computer ab. Die Zukunft vorherzusagen ist bekannterweise nicht einfach, aber wir orientieren uns an dem Mooreschen Gesetz. Diesem zufolge verdoppelt sich die Rechenleistung alle 18 Monate, wobei die Kosten für Computer konstant bleiben. Nach wie vielen Jahren kann eine Maschine zur vollständigen Schlüsselsuche von AES-128 für eine Million Euro realisiert werden, mit der die *durchschnittliche* Suchzeit 24 h beträgt? Wir ignorieren bei dieser Abschätzung die Geldinflation.

1.4. Diese Aufgabe beschäftigt sich mit dem Zusammenhang zwischen Passwörtern und Schlüssellängen. Wir betrachten ein Kryptosystem, bei dem der Schlüssel aus einem Passwort gebildet wird.

1. Zunächst betrachten wir ein Passwort bestehend aus 8 Zeichen, wobei jedes Zeichen durch ein ASCII-Symbol dargestellt ist, d. h. 7 Bit pro Zeichen und 128 mögliche Zeichen. Wie groß ist der Schlüsselraum?
2. Wie groß ist die entsprechende Schlüssellänge in Bit?
3. Viele Nutzer wählen nur Kleinbuchstaben als Zeichen, d. h. es gibt nur 26 Möglichkeiten für jedes Zeichen. Wie groß ist der Schlüsselraum und die entsprechende Schlüssellänge (in Bit)?
4. Aus wie vielen Zeichen muss ein Passwort bestehen, damit sich eine effektive Schlüssellänge von 128 Bit ergibt mit:

   a. 7-Bit-Zeichen?
   b. Zeichen, die nur aus Kleinbuchstaben bestehen?

1.5. Viele moderne Kryptoverfahren basieren auf modularer Arithmetik. Aus diesem Grund sollte man im Umgang mit ihr sicher sein. Führen Sie die folgenden Berechnungen ohne Taschenrechner durch:

1. $15 \cdot 29 \bmod 13$
2. $2 \cdot 29 \bmod 13$
3. $2 \cdot 3 \bmod 13$
4. $-11 \cdot 3 \bmod 13$

Die Ergebnisse sollten im Bereich von $0, 1, \ldots,$ (Modul $-$ 1) liegen. Beschreiben Sie kurz den Zusammenhang zwischen den einzelnen Aufgaben.

1.6. Berechnen Sie ohne Taschenrechner:

1. $1/5 \bmod 13$

2. $1/5 \bmod 7$
3. $3 \cdot 2/5 \bmod 7$

1.7. Wir betrachten den Ring $\mathbb{Z}_4$. Stellen Sie eine Tabelle auf, die die Addition aller Ringelemente untereinander beschreibt. Die Tabelle soll die folgende Form haben:

+	0	1	2	3
0	0	1	2	3
1	1	2	$\cdots$	
2	$\cdots$			
3				

1. Berechnen Sie die Multiplikationstabelle für $\mathbb{Z}_4$.
2. Berechnen Sie die Additions- und Multiplikationstabelle für $\mathbb{Z}_5$.
3. Berechnen Sie die Additions- und Multiplikationstabelle für $\mathbb{Z}_6$.
4. In $\mathbb{Z}_4$ und $\mathbb{Z}_6$ gibt es Elemente ohne multiplikative Inverse. Welche Elemente sind das? Warum haben alle Elemente außer der 0 eine Inverse in $\mathbb{Z}_5$?

1.8. Wie lautet die multiplikative Inverse von 5 in $\mathbb{Z}_{11}$, $\mathbb{Z}_{12}$, und $\mathbb{Z}_{13}$? Man kann sie durch Ausprobieren mit oder ohne Computerunterstützung finden.

Bei dieser Aufgabe sieht man, dass die Inverse von dem Ring abhängt, in dem sich die Zahl befindet. Wie man sieht, ändert sich die Inverse, wenn der Modul sich ändert. Von daher ergibt es keinen Sinn, von der Inversen einer Zahl zu sprechen, solange nicht klar ist, was der Modul ist. Diese Beobachtung ist für das RSA-Kryptoverfahren wichtig, welches in Kapitel 7 eingeführt wird. Um multiplikative Inverse effizient für große Moduln zu berechnen, wird zumeist der euklidische Algorithmus eingesetzt, der in Abschnitt 6.3 behandelt wird.

1.9. Berechnen Sie x so weit wie möglich ohne Taschenrechner. Es ist empfehlenswert, Zwischenergebnisse mit dem Modul zu reduzieren, wie in dem Beispiel in Abschnitt 1.4.1 gezeigt wurde:

1. $x = 3^2 \bmod 13$
2. $x = 7^2 \bmod 13$
3. $x = 3^{10} \bmod 13$
4. $x = 7^{100} \bmod 13$
5. $7^x = 11 \bmod 13$

In der letzten Aufgabe wird ein sogenannter diskreter Logarithmus berechnet, der in Kapitel 8 eingehend behandelt wird. Viele moderne asymmetrische Kryptoverfahren, beispielsweise der Schlüsselaustausch nach Diffie-Hellman, basieren auf dem diskreten Logarithmus, wobei allerdings Zahlen mit einer Länge von 2000 Bit oder mehr verwendet werden sollten.

1.10. Bestimmen Sie alle natürlichen Zahlen n zwischen $0 \leq n < m$, die teilerfremd zu m sind, wobei $m = 4, 5, 9, 26$. Es gibt ein spezielles Symbol für die *Anzahl* der Zahlen n, die diese Bedingung erfüllen. Man schreibt dann $\phi(m)$. Zum Beispiel gilt $\phi(3) = 2$, da sowohl 1 als auch 2 teilerfremd zu dem Modul 3 sind. Die Funktion $\phi(m)$ heißt eulersche Phi-Funktion. Bestimmen Sie $\phi(m)$ für $m = 4, 5, 9, 26$.

1.11. Diese Aufgabe betrachtet die affine Chiffre mit dem Schlüssel $a = 7$, $b = 22$.

1. Entschlüsseln Sie den Geheimtext:
   `falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj`
2. Von wem stammt der Satz?

1.12. Wir verallgemeinern nun die affine Chiffre aus Abschnitt 1.4.4 für das vollständige deutsche Alphabet, d. h. der Klartext- und Chiffratraum umfassen neben den 26 regulären Buchstaben auch die Umlaute Ä, Ö, Ü sowie das ß. Es wird die folgende Codierung verwendet:

A $\leftrightarrow$ 0	B $\leftrightarrow$ 1	C $\leftrightarrow$ 2	D $\leftrightarrow$ 3	E $\leftrightarrow$ 4	F $\leftrightarrow$ 5
G $\leftrightarrow$ 6	H $\leftrightarrow$ 7	I $\leftrightarrow$ 8	J $\leftrightarrow$ 9	K $\leftrightarrow$ 10	L $\leftrightarrow$ 11
M $\leftrightarrow$ 12	N $\leftrightarrow$ 13	O $\leftrightarrow$ 14	P $\leftrightarrow$ 15	Q $\leftrightarrow$ 16	R $\leftrightarrow$ 17
S $\leftrightarrow$ 18	T $\leftrightarrow$ 19	U $\leftrightarrow$ 20	V $\leftrightarrow$ 21	W $\leftrightarrow$ 22	X $\leftrightarrow$ 23
Y $\leftrightarrow$ 24	Z $\leftrightarrow$ 25	Ä $\leftrightarrow$ 26	Ö $\leftrightarrow$ 27	Ü $\leftrightarrow$ 28	ß $\leftrightarrow$ 29

1. Wie lauten die Ver- und Entschlüsselungsgleichung der Chiffre?
2. Wie groß ist der Schlüsselraum?
3. Das folgende Chiffrat wurde mit dem Schlüssel $(a = 17, b = 1)$ erzeugt. Bestimmen Sie den Klartext.

   `ä u ß w ß`

4. Aus welchem Dorf stammt der Klartext?

1.13. Bei einer sogenannten *chosen plaintext attack* ist der Angreifer, Oskar, in der Lage, Klartexte zu wählen und diese von Alice verschlüsseln zu lassen. Dies kann in der Praxis beispielsweise vorkommen, wenn Alice ein Webserver ist, der Eingabedaten verschlüsselt versendet.

Zeigen Sie, wie Oskar die affine Chiffre brechen kann, wenn er zwei Klartext-Chiffrat-Paare (x_1, y_1) und (x_2, y_2) kennt, wobei Oskar x_1 und x_2 gewählt hat. Welche Bedingung müssen x_1 und x_2 erfüllen?

1.14. Ein naheliegender Ansatz, um die Sicherheit symmetrischer Chiffren zu erhöhen, ist es, eine Nachricht zweimal zu verschlüsseln:

$$y = e_{k_2}(e_{k_1}(x))$$

In der Kryptografie gibt es jedoch oft Fallstricke und es ist leicht, Lösungen zu entwerfen, die nur scheinbar sicher sind. In dieser Aufgabe zeigen wir, dass die Doppelverschlüsselung mit der affinen Chiffre nur so sicher ist wie eine Einfachverschlüsselung.

Wir betrachten zwei affine Chiffren $e_{k1} \equiv a_1 x + b_1 \bmod 26$ und $e_{k2} \equiv a_2 x + b_2 \bmod 26$.

1. Zeigen Sie, dass es eine einzelne affine Chiffre $e_{k3} \equiv a_3 x + b_3 \bmod 26$ gibt, die genau die gleiche Ver- und Entschlüsselung ausführt wie die Doppelverschlüsselung $e_{k2}(e_{k1}(x))$.

2. Bestimmen Sie die Werte a_3 und b_3 für $a_1 = 3, b_1 = 5$ und $a_2 = 11, b_2 = 7$.
3. Zur Verifikation der Lösung verschlüsseln Sie den Buchstaben `K` (i) zunächst mit e_{k_1} und das resultierende Chiffrat dann mit e_{k_2} und (ii) verschlüsseln Sie `K` mit e_{k_3}.
4. Beschreiben Sie eine effiziente Methode, um eine vollständige Schlüsselsuche gegen die affine Chiffre mit Doppelverschlüsselung durchzuführen. Ändert sich der effektive Schlüsselraum?

Bemerkung: Mehrfachverschlüsselung kann sehr wohl die Sicherheit einer Chiffre erhöhen. Ein prominentes Beispiel ist DES (Data Encryption Standard). Der einfache DES ist sehr unsicher, DES mit Dreifachverschlüsselung (3DES) jedoch sehr sicher. Er wird z. B. im deutschen elektronischen Personalausweis oder im biometrischen Reisepass eingesetzt. Mehr Informationen zu 3DES finden sich in Abschnitt 3.7.2.