AUFGABEN ZUR KRYPTOLOGIE

Aufgabe 1

Der folgende Geheimtext ging hervor aus der Verschlüsselung eines deutschen Klartexts mit einem monoalphabetischen Chiffrierungsverfahren.

```
nyv syv svdvu yst vyuv sglmdv avtdgrv uymdt svdw symdvw xur jiuu
wvlityc vyueimd hvbwgmdvu nvwrvu
```

Versuchen Sie, den Geheimtext zu brechen, d.h. den Klartext herauszufinden. Um Ihnen die Arbeit zu erleichtern, gibt die nachfolgende Tabelle die Häufigkeit der häufigsten Buchstaben und Bigramme im Geheimtext an.

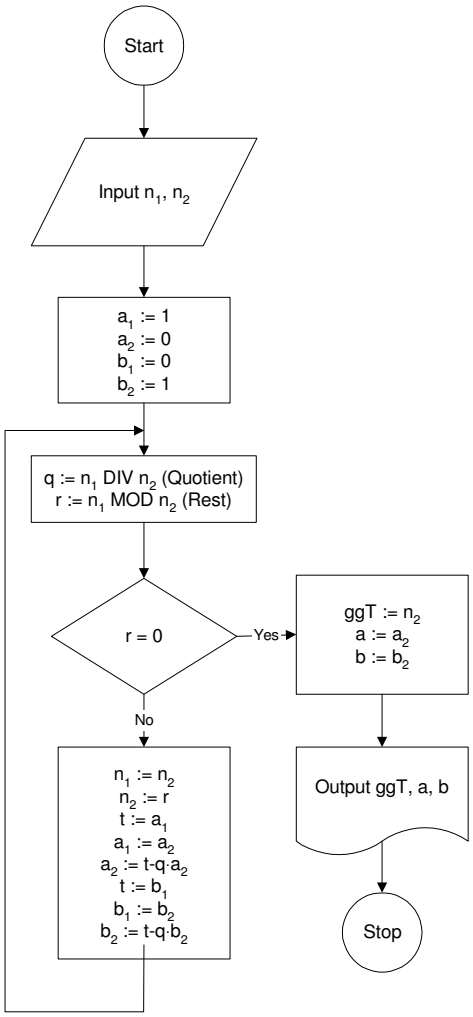
Buchstabe	Anzahl	Bigramm	Anzahl
v	17	md	5
u	9	dv	4
y	8	vu	3
d	8	yv	2
s	6	yu	2
w	5	ym	2
m	5	vy	2
t	4	vw	2
r	3	vl	2
i	3	vd	2
g	3	uv	2
n	2	sy	2
l	2	sv	2
		rv	2

Aufgabe 2

Falls n_1 und n_2 zwei ganze Zahlen mit dem grössten gemeinsamen Teiler $ggT(n_1,n_2)$ sind, so gibt es immer zwei ganze Zahlen a und b, so dass gilt

$$ggT(n_1,n_2) = a \cdot n_1 + b \cdot n_2$$

Sowohl der grösste gemeinsame Teiler als auch die Faktoren a und b lassen sich mit Hilfe des erweiterten Euklidschen Algorithmus sehr effizient bestimmen.



1. Suchen Sie den ggT von 132 und 128 sowie die beiden ganzen Zahlen a und b, so dass ggT(132,128) = a·132 + b·128. Verwenden Sie dazu die nachfolgende Tabelle.

n_1	n_2	a_1	a_2	b_1	b_2	q	r
132	128	1	0	0	1		

Beim RSA-Algorithmus sind $\Phi(n) = (p - 1)(q - 1)$ und der öffentliche Schlüssel e teilerfremd, d.h. der grösste gemeinsame Teiler ist 1. Es existieren also zwei ganze Zahlen a und b, so dass $1 = a \cdot \Phi(n) + b \cdot e$, welche mit dem erweiterten Euklidschen Algorithmus gefunden werden können. Diese Gleichung gilt auch dann noch, wenn nur der Rest betrachtet wird, der sich bei Division durch $\Phi(n)$ ergibt:

$$1 \bmod \Phi(n) = \left[a \cdot \Phi(n) + b \cdot e\right] \bmod \Phi(n)$$

2. Wie kann diese Beziehung dazu ausgenützt werden, um den geheimen Schlüssel d des RSA-Verfahrens zu bestimmen?
3. Gegeben sind die beiden Primzahlen p = 13 und q = 17 sowie der öffentliche Schlüssel e = 5. Berechnen Sie den geheimen Schlüssel d.

Aufgabe 3

1. Wieviel Multiplikationen benötigen Sie, um eine Zahl a mit 65537 zu potenzieren, d.h. um a^{65537} zu berechnen?

   Tipp: $65537 = 2^{16} + 1$

2. Wieviel Multiplikationen sind maximal notwendig, falls der Exponent eine Zahl mit L Binärstellen ist?

Aufgabe 4

Wir bezeichnen den Rest, der sich bei Division von n durch d ergibt mit $R_d(n)$.

Welche Beziehungen gelten zwischen $R_d(n_1)$, $R_d(n_2)$ und

a) $R_d(n_1 + n_2)$

b) $R_d(n_1 \cdot n_2)$

Aufgabe 5

Ordnen Sie den folgenden Tätigkeiten und Objekten die Begriffe „Vertraulichkeit“, „Authentikation“ und „Integrität“ zu.

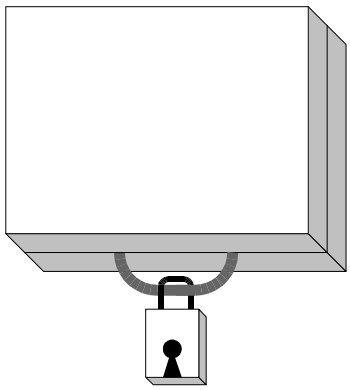
- Rose im Knopfloch
- Brief in Umschlag stecken und zukleben
- Fingerabdruck
- Briefsiegel
- Unterschrift

Aufgabe 6

Erklären Sie das Prinzip der asymmetrischen Verschlüsselungsverfahren anhand von Briefen welche in mit Namensschildern versehene Briefkästen gesteckt werden.

Aufgabe 7

Alice und Bob verwenden einen mit Schlössern verschliessbaren Koffer um geheime Nachrichten auszutauschen.



1. Wie können Alice und Bob dies bewerkstelligen, ohne dass sie die Schlüssel ihrer Schlösser austauschen müssen? Welche Voraussetzungen müssen an den Koffertransportweg gestellt werden?
2. Das „Abschliessen“ einer Nachricht m durch den Teilnehmer T werde mathematisch durch das Berechnen von $m^{e_T} \bmod p$ nachgebildet (p: öffentliche Primzahl > m). Wie könnte in diesem Fall die elektronische Form des obigen Protokolls aussehen?

Aufgabe 8

1. Versuchen Sie die Zahl 14803 ohne Verwendung des Taschenrechners zu faktorisieren.
2. Die Zahl 14803 ist das Produkt zweier Primzahlen und $\Phi(14803) = 14560$. Können Sie nun die Faktorisierung durchführen?

Aufgabe 9

Der öffentliche Schlüssel eines RSA-Systems sei mit n = 247 und e = 7 gegeben.

a) Verschlüsseln Sie die Nachricht m = 10.

b) Verschlüsseln Sie die Nachricht m = 100 = 10^2.

c) Knacken Sie den Code, indem Sie den geheimen Schlüssel d bestimmen.

d) Sie empfangen die verschlüsselte Nachricht c = 2. Wie lautet der entsprechende Klartext?

Aufgabe 10

Beim RSA-Verfahren sei der öffentliche Schlüssel bekannt: n = 10, e = 3.

a) Verschlüsseln Sie die Nachricht m = 3.

b) Bestimmen Sie den geheimen Schlüssel d (Zur Erinnerung: $e \cdot d \bmod \phi(n) = 1$).

c) Verifizieren Sie den geheimen Schlüssel, indem Sie die verschlüsselte Nachricht wieder entschlüsseln.

d) Der Chiffrierschlüssel werde nun auf e = 2 geändert. Verschlüsseln Sie die Nachrichten $m_1 = 4$ und $m_2 = 6$. Erläutern Sie das Ergebnis.

Aufgabe 11

Im nachfolgenden seien p_1, p_2, ... ungleiche Primzahlen. Geben Sie für die folgenden Argumente m jeweils einen Ausdruck zur Berechnung der Eulerschen Funktion $\Phi(m)$ an.

a) $m = p_1^2$

b) $m = p_1^n$

c) $m = p_1^2 \cdot p_2$

d) $m = p_1 \cdot p_2 \cdot p_3$

Aufgabe 12

Gegeben ist ein öffentlicher RSA-Schlüssel mit dem Modul n = 143 und dem Exponenten e = 11.

a) Ist die Wahl des Exponenten zulässig (einmal abgesehen von seiner Länge)? Mit Begründung!

b) Bestimmen Sie den zur Nachricht m = 60 gehörenden Geheimtext.

c) Brechen Sie die Verschlüsselung, indem Sie den geheimen Schlüssel d bestimmen.

Aufgabe 13

Füllen Sie die nachfolgende Tabelle aus.

Achtung: Falsch gesetzte Kreuze ergeben einen Abzug!

	IDEA	DES	AES	Triple DES
Beinhaltet ein Feistel-Netzwerk	❑ ja ❑ nein	❑ ja ❑ nein	❑ ja ❑ nein	
Gilt als sicher	❑ ja ❑ nein	❑ ja ❑ nein	❑ ja ❑ nein	❑ ja ❑ nein
Schlüssellänge in Bit				
Blocklänge in Bit				
Anzahl Runden				

Aufgabe 14

Zum Abspeichern von Passworten wird gelegentlich das folgende Verfahren vorgeschlagen:

Jedem Passwort wird ein zufällig gewählter Wert (salt) angehängt und die daraus resultierende Zeichenkette wird anschliessend in einer Einweg-Funktion verrechnet. In der Passwortdatei werden das Ergebnis der Einweg-Funktion und der zufällig gewählte Wert abgelegt.

a) Wie wird beim Einloggen die Gültigkeit des eingegeben Passwortes überprüft?

b) Ergeben sich durch das beschriebene Verfahren Vorteile, obwohl der zufällig gewählte Wert im Klartext abgespeichert und deshalb einem Angreifer bekannt ist? Falls ja, welche?

Aufgabe 15

Nennen Sie drei Gründe, weshalb bei IDEA die Blocklänge der internen Rechenoperationen mit 16 Bit gewählt wurde.

Aufgabe 16

Es scheint praktisch unmöglich zu sein, aus der Analyse von Coca Cola auf das Rezept zu schliessen. Andererseits ist es offensichtlich auch nicht möglich, mit einem anderen Rezept ein zu Coca Cola identisches Getränk zu produzieren.

a) Nennen Sie einen kryptologischen Begriff, der vergleichbare Eigenschaften aufweist.

Aufgabe 17

Die Zahl $\pi(n)$ der Primzahlen unterhalb von n ist für grosse n näherungsweise durch

$$\pi(n) \approx \frac{n}{\ln(n)}$$

gegeben.

a) Wie viele Primzahlen gibt es mit einer maximalen Länge von 512 Bit?

b) Nehmen Sie an, diese Primzahlen würden auf einer Festplatte gespeichert, die pro Gramm Masse 1 GByte Daten speichern kann. Wie schwer wäre diese Festplatte?

c) Die Masse eines schwarzen Lochs liegt in der Grössenordnung 10^{31} kg. Vergleichen Sie das Resultat aus b) mit dieser Zahl.

Aufgabe 18

Statistischer Primzahlentest

Sei n eine ungerade Zahl für die auch (n – 1)/2 ungerade ist. Dann gilt

1. n prim $\Rightarrow a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$ für alle a ∈ {1, 2, ..., n-1}

2. n nicht prim $\Rightarrow a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$ für höchstens die Hälfte der a ∈ {1, 2, ..., n-1}

Daraus lässt sich der folgende statistische Primzahlentest ableiten

1. Wähle Zufallszahlen $a_1, a_2, ..., a_k$ aus {1, 2, ..., n-1}
2. Berechne $a_k^{\frac{n-1}{2}} \bmod n$
3. Falls alle Ergebnisse gleich ±1 sind, entscheide n ist prim, sonst n nicht prim.

a) Wenden Sie das Verfahren auf n = 23 und n = 15 an.

b) Wie gross ist die Wahrscheinlichkeit für einen Fehlentscheid?

Aufgabe 19

Gegeben sei N = 77. Wählen Sie eine beliebige Zahl a aus der Menge {1, 2, ..., N-1}, welche N nicht teilt. (Tipp: a nicht zu gross wählen).

a) Berechnen Sie $f(x) = a^x \bmod N$ für x = 1, 2, 3, ...

b) Bezeichnen Sie die Periode von f(x) mit r und berechnen Sie $p = ggT(a^{r/2}+1,N)$ und $q = ggT(a^{r/2}-1,N)$.

c) Fällt Ihnen etwas auf?

Bemerkung: Leider ist die Bestimmung der Periode genau so aufwändig wie die Faktorisierung von N.

Aufgabe 20

Chinesisches Restwert-Theorem

Gegeben seien positive ganze Zahlen m_1, m_2, m_k, die jeweils paarweise teilerfremd sind, d.h. $ggT(m_i, m_j) = 1$ für $i \neq j$. Dann hat das Gleichungssystem

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_k \bmod m_k \end{aligned}$$

eine ganzzahlige Lösung, welche in der Menge $\{0, 1, ..., m_1 \cdot m_2 \cdot ... m_k - 1\}$ eindeutig ist.

Beispiel: Das Gleichungssystem

$$\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 3 \bmod 5 \\ x &\equiv 2 \bmod 7 \end{aligned}$$

ist für x = 23 erfüllt. Diese Lösung ist die einzige im Bereich 0..104.

Die Lösung x lässt sich wie folgt berechnen. Sei $m = m_1 \cdot m_2 \cdot ... m_k$, $M_i = m/m_i$ und $N_i = M_i^{-1} \bmod m_i$. Dann gilt

$$x = \left(\sum_{i=1}^{k} a_i \cdot N_i \cdot M_i \right) \bmod m$$

a) Lösen Sie das folgende Gleichungssystem:

$$\begin{aligned} x &\equiv 1 \bmod 2 \\ x &\equiv 3 \bmod 5 \\ x &\equiv 4 \bmod 7 \end{aligned}$$

Aufgabe 21

(Aus der Vorlesung „Informationssicherheit und Kryptographie“ von Prof. U. Maurer, ETH Zürich)

a) Sie erhalten die mit RSA verschlüsselte Nachricht y = 7, wobei n = 899 und e = 11 verwendet wurde. Wie lautet der Klartext? Warum kann bei diesem n für e nicht ein kleinerer Wert als 11 verwendet werden?

Tipps für die Rechnung: $a \cdot 11 + b \cdot 840 = 1$ kann man für b = -8 erfüllen. Zudem gilt $7^{210} \equiv 1 \bmod 899$ und $7^{401} \equiv 20 \bmod 899$.

b) Kann RSA auch verwendet werden, wenn der Modulus mehr als zwei Primfaktoren besitzt? Geben Sie je ein Argument für und gegen die Verwendung dieser Variante.

c) In einem Netzwerk wird das RSA-System verwendet, wobei jeder Benutzer einen eigenen Modulus veröffentlicht, aber alle den gleichen Exponenten e = 3 verwenden. Zeigen Sie, dass dieses System unsicher ist, wenn die gleiche Nachricht an drei oder mehr verschiedene Benutzer gesendet wird. (Tipp: Chinesischer Restsatz) Klappt diese Attacke auch für e > 3?