

Kryptographie

Aufgabe 1 Zum folgenden durch Transposition entstandenen Geheimtext ist der Klartext gesucht:

RPEOETEDI ETISARUOM ITTMSTRUE

Hinweis Schreiben Sie die Wörter des Geheimtextes untereinander und durchlaufen Sie das so entstandene Rechteckschema auf einem geeigneten Weg.

Bemerkung Für eine natürliche Zahl n bezeichne $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ die Menge der Reste modulo n . Auf $\mathbb{Z}_n$ ist eine Addition und eine Multiplikation erklärt. Sind m und n natürliche Zahlen, so bezeichne $\text{ggT}(m, n)$ den größten gemeinsamen Teiler von m und n .

Aufgabe 2 Rechnen Sie modulo 12; dabei können Sie die Elemente von $\mathbb{Z}_{12}$ mit der Uhrzeit identifizieren. Beispielsweise wird ein Zug, der um 11 Uhr abfährt und 2 Stunden fährt, um 1 Uhr ankommen, also $11 + 2 = 1 \pmod{12}$.

$$0 + 3; \quad 4 + 8; \quad 3 \cdot 8; \quad 3^3.$$

Aufgabe 3 a) Sei $n \in \mathbb{N}$ und sei $t \in \{2, \dots, n-1\}$ derart, daß $\text{ggT}(t, n) > 1$. Zeigen Sie: Es gibt ein $x \in \{1, 2, \dots, n-1\}$, so daß $t \cdot x = 0 \pmod{n}$ gilt.

b) Sei $n \in \mathbb{N}$ und sei $t \in \{1, 2, \dots, n-1\}$ mit $\text{ggT}(t, n) = 1$. Man zeige: die Abbildung $f_t : \mathbb{Z}_n \rightarrow \mathbb{Z}_n, x \mapsto t \cdot x \pmod{n}$ ist bijektiv.

c) Ein Element $x \in \mathbb{Z}_n$ heißt Einheit, falls es ein $y \in \mathbb{Z}_n$ gibt mit $x \cdot y = 1 \pmod{n}$. Welche Elemente in $\mathbb{Z}_n$ sind Einheiten?

Aufgabe 4 Erstellen Sie eine Additionstabelle und eine Multiplikationstabelle für $\mathbb{Z}_7$ und $\mathbb{Z}_8$.

Aufgabe 5 Wie viele verschiedene Schlüssel für Tauschchiffren gibt es über einem Alphabet mit n Buchstaben

a) im Falle $n = 12$?

b) im Falle $n = 13$?

Kryptographie

Aufgabe 6 Welche der folgenden Abbildungen $f : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$ sind zulässige Tauschchiffren? Finden Sie gegebenenfalls die zugehörige Umkehrabbildung.

- a) $f(x) = 13 \cdot x + 4 \bmod 26$;
- b) $f(x) = 21 \cdot x + 2 \bmod 26$;
- c) $f(x) = 7 \cdot x \bmod 26$.

Aufgabe 7 Wir betrachten folgendes Chiffrierverfahren: Die zu verschlüsseln- den Texte und ebenso die zu verwendenden Schlüssel seien Folgen von 6 Buch- staben des deutschen Alphabets. Unter den (6-stelligen) Klartext schreibt man das (6-stellige) Schlüsselwort. Der unter dem jeweiligen Klartextbuchsta- ben stehende Buchstabe des Schlüsselworts bestimmt dann die zu verwendende Verschiebechiffrierung.

- a) Welcher Geheimtext ergibt sich für den Klartext SOMMER bei Verwendung des Schlüsselwortes HERBST?
- b) Es wurde das Schlüsselwort HERBST verwendet und der Geheimtext ENF- VXL empfangen. Wie lautet der zugehörige Klartext?
- c) Stellen Sie das oben beschriebene Chiffrierverfahren als Kryptosystem - $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ im Sinne der Definition aus der Vorlesung dar.

Aufgabe 8 Es seien $(\Omega, \mathcal{S}, P)$ ein Wahrscheinlichkeitsraum sowie $A, B, C \in \mathcal{S}$ Er- eignisse mit $P(A|C) = 0.5$, $P(A|\bar{C}) = 0.0$, $P(B|\bar{C}) = 0.6$, $P(\bar{B}|C) = 0.4$, $P(C) = 0.3$.

- a) Man bestimme $P(A)$ und $P(B)$
- b) Man überprüfe, ob A und C bzw. B und C unabhängige Ereignisse bezüg- lich P sind.

Hinweis zu a) Formel von der totalen Wahrscheinlichkeit.

Aufgabe 9 Bei der Übertragung der Zeichen "Punkt" und "Strich" in einem Fernmeldesystem werden durch Störungen im Mittel 5% der gesendeten Punk- te als Striche und 3% der gesendeten Striche als Punkte empfangen. Das Ver- hältnis von gesendeten Punkten zu gesendeten Strichen ist 4:5. Wie groß ist die Wahrscheinlichkeit, daß das richtige Zeichen empfangen wurde, falls "Punkt" empfangen wurde?

Kryptographie

Aufgabe 10 Gegeben sei das Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ mit $\mathcal{P} = \{0, 1\}$, $\mathcal{C} = \{a, b\}$ und $\mathcal{K} = \{A, B\}$. Weiter seien die Wahrscheinlichkeitsverteilungen $P_{\mathcal{P}}$ mit $P_{\mathcal{P}}(0) = \frac{1}{4}$, $P_{\mathcal{P}}(1) = \frac{3}{4}$ und $P_{\mathcal{K}}$ mit $P_{\mathcal{K}}(A) = \frac{1}{4}$, $P_{\mathcal{K}}(B) = \frac{3}{4}$ gegeben sowie die Verschlüsselungsfunktionen E_k , $k \in \mathcal{K}$, mit

$$E_A(0) = a, E_A(1) = b, E_B(0) = b, E_B(1) = a.$$

Klartext- und Schlüsselwahl seien stochastisch unabhängig.

- a) Zeigen Sie anhand der Definition, daß dieses Kryptosystem nicht perfekt sicher ist.
- b) Wie muß man $P_{\mathcal{K}}(A)$ und $P_{\mathcal{K}}(B)$ wählen, um $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ perfekt sicher zu machen?

Aufgabe 11 Entschlüsseln Sie den folgenden Text, von dem Sie wissen, dass er mit einer Verschiebechiffre $f : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$, $x \mapsto x + s \bmod 26$ verschlüsselt wurde (das deutsche Alphabet wird mit $\mathbb{Z}_{26}$ identifiziert). Finden Sie s .

PXPXKXENVDRUXVTNLXHYMXGMAXYKXJN

XGVRFXMAHWGXXWLEHGZXKVBIAKMXQM

Hinweis: Häufigkeitsanalyse.

Aufgabe 12 Der folgende Geheimtext wurde mit der Tauschchiffre $f : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$, $x \mapsto 3x + 7 \bmod 26$ verschlüsselt. Finden Sie den Klartext.

LCHZW

Aufgabe 13 Der untenstehende Geheimtext wurde mit einer sogenannten Vigenère-Chiffre verschlüsselt: Unter den Klartext wird fortlaufend ein Schlüsselwort geschrieben. Der jeweilige Buchstabe des Schlüsselwortes bestimmt die Verschiebechiffre für den zugehörigen Klartextbuchstaben: steht z. B. unter einem U ein K, so wird für das U ($=21$) die Verschiebechiffre mit $s = 11$ ($=K$) angewendet, also $U \rightarrow 21 + 11 = 6 \bmod 26 = F$. Das Schlüsselwort ist der Klartext aus Aufgabe 12. Entschlüsseln Sie:

NCCTLMUEDFFYAVSAURBNNXJAHXDVJSLINCG

BUBXQAURCPXIBTFXIETFYQQGSGQDHRXDTTB

Kryptographie

Bemerkung Ein häufig verwendetes Alphabet ist der ASCII-Zeichensatz. Er umfasst 256 Zeichen, die durch die Zahlen $0, 1, \dots, 255$ codiert werden. Wir geben einen kurzen Auszug aus der ASCII-Tabelle:

32		65	A	66	B
67	C	68	D	69	E
70	F	71	G	72	H
73	I	74	J	75	K
76	L	77	M	78	N
79	O	80	P	81	Q
82	R	83	S	84	T
85	U	86	V	87	W
88	X	89	Y	90	Z

Im Computer werden die ASCII-Zeichen als Binärzahlen gespeichert, das heißt die Dezimalzahlen werden in Binärzahlen umgewandelt. Für jedes Zeichen werden 8 Bit gespeichert.

Beispiel: $A \hat{=} (65)_{10} = (1000001)_2$ wird als ASCII-Zeichen folgendermaßen gespeichert: $A \hat{=} 01000001$. Dabei bedeutet der Index 10, dass 65 eine Dezimalzahl ist, der Index 2, dass 1000001 eine Binärzahl ist.

Aufgabe 14 Die folgenden beiden Geheimtexte wurden nach dem Prinzip des Vernam One-Time-Pads verschlüsselt, allerdings wurde zweimal der selbe Schlüssel verwendet:

$$\begin{array}{l} 011000111101010111011111100011011110000011100100 \\ 100001100010110011110110110100100110100011101000 \end{array} \quad (1)$$

$$\begin{array}{l} 011011111101010011011110111010001111001111101000 \\ 100000000010011110010111110000010110001011111000 \end{array} \quad (2)$$

Der Klartext zu Text 1 lautet "ONE TIME PAD". Finden Sie den Klartext zu Text 2.

Hinweis Die Buchstaben des Klartexts wurden gemäß dem ASCII-Zeichensatz als Binärzahlen mit 8 Bit dargestellt.

Aufgabe 15 Bestimmen Sie in $(\mathbb{Z}_{26}, \cdot)$ die von 7 erzeugte Untergruppe $\langle 7 \rangle$.

Kryptographie

Aufgabe 16 Berechnen Sie mit dem euklidischen Algorithmus $ggT(100, 35)$.

Aufgabe 17 Berechnen Sie, falls möglich, den kleinsten nichtnegativen Rest:

a) $4^{-1} \bmod 15$, b) $13^{-1} \bmod 26$, c) $7^{-1} \bmod 15$, d) $5^{-1} \bmod 21$.

Aufgabe 18 Schreiben Sie ein Computer-Programm, das für zwei Zahlen $a, b \in \mathbb{N}_0$ $d := ggT(a, b)$ sowie Zahlen $s, t \in \mathbb{Z}$ mit $d = s \cdot a + t \cdot b$ berechnet.

Hinweis Die Folgen $(r_i)_{i \in \mathbb{N}}$, $(q_i)_{i \in \mathbb{N}}$ seien wie in Satz 2.3 definiert und es gelte $ggT(a, b) = r_{n+1}$ für ein $n \in \mathbb{N}$. Definiere

$$x_1 := 1, x_2 = 0, y_1 = 0, y_2 = 1,$$

$$x_{k+1} = q_{k-1}x_k + x_{k-1}, \quad y_{k+1} = q_{k-1}y_k + y_{k-1}, \quad 2 \leq k \leq n+1.$$

Dann gilt

$$r_k = (-1)^{k+1}x_ka + (-1)^ky_kb \quad \text{für } 1 \leq k \leq n+1.$$

Aufgabe 19 Sie wollen durch *Probedivision* nachweisen, dass die Zahl $n \in \mathbb{N}$ eine Primzahl ist, das heißt Sie testen für die Zahlen $2, 3, \dots$ ob sie n teilen. Wann können sie sicher sein, dass n prim ist?

Aufgabe 20 Zerlegen Sie die Zahlen 2002 und 2003 in ihre Primfaktoren.

Kryptographie

Aufgabe 21 Wir betrachten das folgende Alphabet:

	0	A	1	C	2	D	3	E	4
G	5	H	6	I	7	L	8	M	9
N	10	R	11	S	12	T	13	!	14
=	15	/	16	?	17	%	18	\$	19

Das RSA-Verfahren wird mit diesem Alphabet ausgeführt. n bezeichnet den RSA-Modul, e den Verschlüsselungsexponenten.

- a) Senden Sie dem Empfänger mit dem öffentlichen Schlüssel $(n, e) = (21, 5)$ verschlüsselt folgende Nachricht: "DATEI ERHALTEN".
- b) Entschlüsseln Sie folgende Nachricht. Ihr öffentlicher Schlüssel lautet $(n, e) = (21, 5)$.

%ACD%/\$DRH ?/DIRHT/T!

Aufgabe 22 Wir betrachten das RSA-Verfahren mit dem RSA-Modul $n = 22663$. Es gilt $\varphi(n) = 22360$.

- a) Finden Sie die Primfaktorzerlegung von n ohne Hilfe eines Computers.
- b) Ihr öffentlicher Schlüssel sei $e = 14907$. Berechnen Sie Ihren privaten Schlüssel d .
- c) Gegeben ist folgendes Alphabet:

	0	A	1	B	2	C	3	D	4	...	Z	26
--	---	---	---	---	---	---	---	---	---	-----	---	----

Vor der Verschlüsselung wird der Klartext in Blöcke der Länge 2 unterteilt und als Zahl zur Basis 27 dargestellt.

Beispiel: KR $\hat{=}$ 11 18 $\leftrightarrow$ $11 \cdot 27 + 18 = 297 + 18 = 315$

Nach diesem Prinzip wurde der folgende Text verschlüsselt

3595 10898 2212 4379 1736 14519 6584 2489 21854 15215 4972 12974

Entschlüsseln Sie ihn mit Ihrem privaten Schlüssel d .

Kryptographie

Aufgabe 23 Betrachten Sie die Abbildung $e_3 : \mathbb{Z}_{15} \rightarrow \mathbb{Z}_{15}$, $x \mapsto x^3 \bmod 15$. Überzeugen Sie sich davon, dass e_3 bijektiv ist, indem Sie $e_3(x)$ für alle $x \in \mathbb{Z}_{15}$ berechnen. Wie ist der Exponent k zu wählen, dass $d_k : \mathbb{Z}_{15} \rightarrow \mathbb{Z}_{15}$, $x \mapsto x^k \bmod 15$ die Umkehrabbildung von e_3 ist?

Aufgabe 24 Wir betrachten das RSA-Verfahren mit dem RSA-Modul 55. Geben Sie alle zulässigen Verschlüsselungsexponenten an.

Aufgabe 25 Der Klartext, der mit dem RSA-Verfahren mit Modul n verschlüsselt werden soll, besteht aus Zeichen des folgenden Alphabets mit 27 Buchstaben:

	0	A	1	B	2	C	3	D	4	...	Z	26
--	---	---	---	---	---	---	---	---	---	-----	---	----

Eine Folge $m_1, \dots, m_k$ von k Buchstaben dieses Alphabets wird als Zahl zur Basis 27 geschrieben gemäß

$$m = \sum_{i=1}^k m_i 27^{k-i}.$$

Dann wird m mit dem RSA-Verfahren verschlüsselt, d. h. der Geheimtext c wird mit dem Verschlüsselungsexponenten e folgendermaßen berechnet:

$$c = m^e \bmod n.$$

Wie groß dürfen wir k wählen?

Aufgabe 26 Wir betrachten die Menge $\mathbb{Z}_{13}^* = \mathbb{Z}_{13} \setminus \{0\}$ mit der Multiplikation $\cdot : \mathbb{Z}_{13}^* \times \mathbb{Z}_{13}^*$, $a \cdot b \mapsto ab \bmod 13$.

a) Wählen Sie aus der Menge $\{3, 6, 13\}$ ein erzeugendes Element g von $\mathbb{Z}_{13}^*$ aus und berechnen Sie g^x für alle $x \in \mathbb{Z}_{13}^*$.

b) Berechnen Sie falls möglich die folgenden diskreten Logarithmen in $\mathbb{Z}_{13}^*$: $\log_{11}(12)$, $\log_7(3)$, $\log_3(6)$.

Kryptographie

Aufgabe 27 Es liegt das symmetrische Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ vor mit $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0, 1\}^5$, $e_k(p) = p + k$, $d_k(c) = c + k$ jeweils komponentenweise mod 2 für alle $p \in \mathcal{P}, k \in \mathcal{K}, c \in \mathcal{C}$. Wir betrachten das ElGamal-Verschlüsselungsverfahren bzgl. der multiplikativen Gruppe $\mathbb{Z}_{29}^* = \mathbb{Z}_{29} \setminus \{0\}$ mit dem erzeugenden Element $g = 2$. (Jedem Element in $\mathbb{Z}_{29}^*$ ist als Schlüssel seine Binärdarstellung in $\mathcal{K}$ zuzuordnen.)

Empfänger A hat den geheimen Schlüssel $t = 7$. Wie lautet sein öffentlicher Schlüssel τ ? Sender B mit dem geheimen Schlüssel $a = 17$ möchte A den Klartext $p = 10111$ übermitteln. Welchen Geheimtext c und welche Zusatzinformation α schickt B an A ? Wie wird c von A entschlüsselt?

Bemerkung zur additiven Verknüpfung zweier Punkte einer elliptischen Kurve: Sei p eine Primzahl größer als 3, seien $a, b \in \mathbb{Z}_p$ mit $\frac{a^3}{27} + \frac{b^2}{4} \neq 0$ und sei $E = E(p, a, b)$ die elliptische Kurve mit dem unendlich fernen Punkt O , deren endlicher Teil aus den Lösungen $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ der Gleichung $y^2 = P(x) \bmod p$ besteht, wobei $P(x) = x^3 + ax + b \bmod p$.

Seien $A_1 = (x_1, y_1)$ und $A_2 = (x_2, y_2)$ zwei endliche Punkte auf E und sei $A_3 = A_1 \oplus A_2$. A_3 kann dann wie folgt berechnet werden, wobei alle Verknüpfungen als Verknüpfungen im Körper $\mathbb{Z}_p$ zu verstehen sind:

1. **Fall** Sei $A_1 \neq A_2$.

(a) Sei $x_1 \neq x_2$. Setze $m := (y_2 - y_1)(x_2 - x_1)^{-1}$; $x_3 := m^2 - x_1 - x_2$;
 $y_3 := -y_1 - m(x_3 - x_1)$; $A_3 := (x_3, y_3)$.

(b) Sei $x_1 = x_2$. $A_3 := O$

2. **Fall** Sei $A_1 = A_2$.

(a) Sei $y_1 = 0$. $A_3 := O$

(b) Sei $y_1 \neq 0$. Setze $m := P'(x_1)(2y_1)^{-1}$; $x_3 := m^2 - 2x_1$;
 $y_3 := -y_1 - m(x_3 - x_1)$; $A_3 := (x_3, y_3)$. Dabei ist $P'(x) = 3x^2 + a \bmod p$.

Aufgabe 28 Geben Sie alle Elemente der elliptischen Kurve $E = E(7, 1, 1)$ an und erstellen Sie (mit Hilfe der Formeln aus der Bemerkung) eine Verknüpfungstafel für die additive Gruppe $(E(7, 1, 1), \oplus)$. Welche Elemente sind erzeugende Elemente? Bestimmen Sie den diskreten Logarithmus bezüglich $g = (0, 1)$ für jedes Element $x \in E$.

Bitte wenden

Aufgabe 29 Sei G die elliptische Kurve $E(7, 1, 1)$. Die im folgenden auftretenden Operationen $\oplus$ und $-$ beziehen sich auf die in der Gruppe G erklärte Addition. Es liegt das symmetrische Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ vor mit $\mathcal{P} = \mathcal{C} = \mathcal{K} = G$, $e_k(p) = p \oplus k$, $d_k(c) = c - k := c \oplus (-k)$ für alle $p \in \mathcal{P}$, $k \in \mathcal{K}$, $c \in \mathcal{C}$. Wir betrachten das ElGamal-Verschlüsselungsverfahren bzgl. der additiven Gruppe G mit dem erzeugenden Element $g = (0, 1)$. Empfänger A hat den geheimen Schlüssel $t = 4$. Wie lautet sein öffentlicher Schlüssel τ ? Sender B mit dem geheimen Schlüssel $a = 3$ möchte A den Klartext $p = (2, 2)$ übermitteln. Welchen Geheimtext c und welche Zusatzinformation α schickt B an A ? Wie wird c von A entschlüsselt?