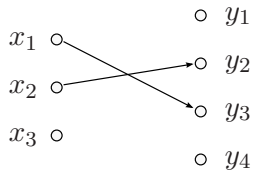
1. Übungsblatt
Kryptographie und Mediensicherheit (SoSe 2018)

Bauhaus-Universität Weimar, Professur für Mediensicherheit (Prof. Lucks)
Betreuer: Eik List
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching`
Abgabe: 17.04.2018, 11 Uhr vor Beginn der Übung oder an `eik.list(at)uni-weimar.de`.
LaTeX-Template: template.tex

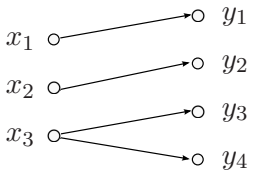
Hinweis: Denken Sie daran, stets nachvollziehbare Lösungswege anzugeben. Für Lösungen, deren Herkunft nicht nachvollziehbar ist, werden 0 Punkte vergeben. Schreiben Sie mindestens eine Matrikelnummer in den Dateinamen Ihrer Abgaben.

Aufgabe 1 – Wiederholung Funktion und Permutation (7 Punkte)
Wiederholen Sie selbständig die Begriffe Funktion, Injektion, Surjektion, Bijektion, Permutation und Transposition. Im Folgenden seien $\mathcal{X} = \{x_1, x_2, \ldots, x_n\}$ und $\mathcal{Y} = \{y_1, y_2, \ldots, y_m\}$ zwei Mengen und $f : \mathcal{X} \to \mathcal{Y}$ eine Funktion.

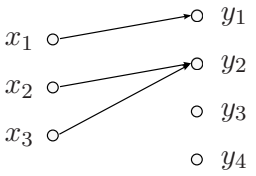
a) Bestimmen Sie für die folgenden Abbildungen, ob es sich um eine Funktion, Injektion, Surjektion, oder Bijektion handelt. Begründen Sie Ihre Antworten.



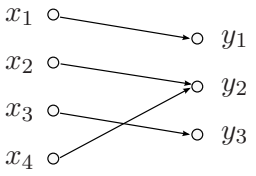
(a1)



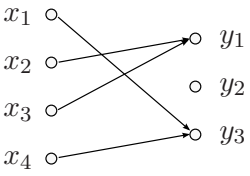
(a2)



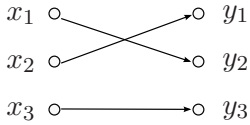
(a3)



(a4)



(a5)



(a6)

b) Kann f eine Bijektion sein, wenn $n < m$? Kann f eine Bijektion sein wenn $n > m$?

c) Seien f und g beliebige Permutationen über $\mathcal{X}$. Zeigen oder widerlegen Sie: $g \circ f$, d. h., die Hintereinanderausführung von $g(f(\cdot))$, ist ebenfalls eine Permutation über $\mathcal{X}$.

d) Sei $f : \mathcal{X} \to \mathcal{X}$ eine Funktion und sei g eine Permutation über $\mathcal{X}$. Zeigen oder widerlegen Sie: $g \circ f$ ist eine Permutation über $\mathcal{X}$.

e) Sei $\{0,1\}^n$ die Menge aller n-bit-Strings. Erhält eine Permutation über $\{0,1\}^n$ stets das Hamming-Gewicht der Eingaben?

Aufgabe 2 – Komplexitätsrechnung (3 Punkte)
Angenommen, Alice besitzt ein Programm das auf ihrem Rechner innerhalb von 4 Minuten 2^{32} Schleifendurchläufe durchläuft.

a) Rechnen Sie hoch, wie viele Durchläufe das Programm innerhalb von 1 Stunde, 1 Tag, 1 Woche, 1 Monat und 1 Jahr schafft.

b) Wie lange bräuchte Alice im Durchschnitt, unter der Annahme aus Teil a), um durch das Ausprobieren aller Schlüssel mit einer Schlüssellänge von 64 bzw. 128 Bits den korrekten zu finden?

Aufgabe 3 – Two-Time Pad (3 Punkte)
Angenommen, die One-Time-Pad-Verschlüsselung der Nachricht "`Sende 100 Euro an Bob`" sei `d549e502c00141953bb7c0a891fa624f44be42a5eb`. Der Klartext ist in 8-Bit-ASCII und der Chiffretext hexadezimal kodiert. Geben Sie den Chiffretext (unter dem gleichen geheimen Schlüssel) zur Nachricht "`Sende 500 Euro an Eve`" an und begründen Sie Ihre Lösung.

Aufgabe 4 – Gruppeneigenschaften (7 Punkte)
Sei $p = 16$. Sei $\mathbb{Z}_p = \{0, \ldots, p-1\}$, $+$ bezeichne die Addition modulo p und $\cdot$ die Multiplikation modulo p.
Wir definieren Klartextmenge, Chiffretextmenge und Schlüsselmenge als $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_p$. Sei $k \in \mathcal{K}$ ein Schlüssel. Wir definieren für alle Nachrichten $m \in \mathcal{M}$ eine Verschlüsselungsfunktion $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ als $E_k(m) \stackrel{\text{def}}{=} (k \cdot m) \bmod p$.

a) Zeigen Sie die Gruppeneigenschaften von $(\mathbb{Z}_{16}, +)$, d. h., ob es ein Gruppoid, eine Halbgruppe, ein Monoid oder eine Gruppe ist und warum. Die Eigenschaften der modularen Addition dürfen Sie als gegeben annehmen.

b) Zeigen Sie die Gruppeneigenschaften von $(\mathbb{Z}_{16}, \cdot)$, d. h., ob es ein Gruppoid, eine Halbgruppe, ein Monoid oder eine Gruppe ist und warum. Die Eigenschaften der modularen Multiplikation dürfen Sie als gegeben annehmen.

c) Definieren Sie eine Entschlüsselungsfunktion $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$ sodass für alle Schlüssel $k \in \mathcal{K}$, alle Nachrichten $m \in \mathcal{M}$ und alle Chiffretexte $c \in \mathcal{C}$ gilt: $D_k(E_k(m)) = m$ und $E_k(D_k(c)) = c$, oder zeigen Sie warum dies nicht möglich ist.

d) Wiederholen Sie Aufgabe c) für $(\mathbb{Z}_{16}, +)$, d. h., $E_k(m) \stackrel{\text{def}}{=} (k + m) \bmod 16$.

e) Wiederholen Sie Aufgabe c) für $(\mathbb{Z}_{17}, \cdot)$, d. h., $E_k(m) \stackrel{\text{def}}{=} (k \cdot m) \bmod 17$.

Aufgabe 5 – Polynom- und Galois-Field-Arithmetik (4 Punkte)
Wiederholen Sie Polynomarithmetik aus Diskrete Strukturen, insbesondere die modulare Multiplikation und Division von Polynomen. Informieren Sie sich selbständig zu Galois Fields, z. B. in der Wikipedia. In der Folge bezeichnen $\mathbb{F}_{p^n}$ oder $\mathbb{GF}(p^n)$ das Galois-Field p^n für eine Primzahl p. Dabei sind alle Elemente $a \in \mathbb{GF}(p^n)$ Polynome vom Grad $< n$ mit Koeffizienten $a_i \in \{0, \ldots, p-1\}$:

$$a(\mathtt{x}) = \sum_{i=0}^{n-1} a_i \cdot \mathtt{x}^i.$$

Wir konzentrieren uns in der Folge auf $\mathbb{GF}(2^n)$. Die Addition entspricht dabei dem bitweisem XOR und die Multiplikation zweier Elemente $a, b \in \mathbb{GF}(2^n)$ entspricht der Polynommultiplikation modulo eines irreduziblen Polynoms $q(\mathtt{x})$ vom Grad n.
Beispiel: Die Elemente von $\mathbb{GF}(2^2)$ sind die Polynome $\{(0 \cdot \mathtt{x} + 0 \cdot \mathtt{1}), (0 \cdot \mathtt{x} + 1 \cdot \mathtt{1}), (1 \cdot \mathtt{x} + 0 \cdot \mathtt{1}), (1 \cdot \mathtt{x} + 1 \cdot \mathtt{1}), \} = \{\mathtt{0}, \mathtt{1}, \mathtt{x}, (\mathtt{x} + \mathtt{1})\}$. Die Koeffizienten a_i sind also Bits. Die Elemente können wir darstellen als String ihrer Koeffizienten a_i, hier die Bitstrings der Länge 2: $\{\mathtt{00}, \mathtt{01}, \mathtt{10}, \mathtt{11}\}$. Das einzige irreduzible Polynom vom Grad 2 ist $q(\mathtt{x}) = \mathtt{x}^2 + \mathtt{x} + 1$.
Die Addition zweier Elemente entspricht dem bitweisen XOR: z. B. $\mathtt{x} + (\mathtt{x} + \mathtt{1}) \equiv (\mathtt{10}) \oplus (\mathtt{11}) = (\mathtt{01})$. Die Multiplikation entspricht der Polynommultiplikation modulo $q(\mathtt{x})$, z. B. $\mathtt{x} \cdot (\mathtt{x} + \mathtt{1}) \bmod q(\mathtt{x}) \equiv \mathtt{1}$:

$$\mathtt{x} \cdot (\mathtt{x} + \mathtt{1}) \bmod (\mathtt{x} + \mathtt{x} + \mathtt{1}) \equiv \mathtt{10} \cdot \mathtt{11} \bmod \mathtt{111} \equiv \mathtt{110} \bmod \mathtt{111} \equiv \mathtt{1}.$$

a) Ermitteln Sie nachvollziehbar ein irreduzibles Polynom $q(\mathtt{x})$ mit binären Koeffizienten a_i vom Grad $n = 3$.

b) Stellen Sie die Multiplikationstabelle aller Elemente im Körper $\mathbb{GF}(2^3)$ mit dem irreduziblem Polynom $q(\mathtt{x})$ aus Aufgabe a) auf.

Aufgabe 6 – E-Mail-Verschlüsselung (Bonus: +1 Punkt)
Für die meisten gängigen E-Mail-Programme (Thunderbird/icedove, Outlook, ...) gibt es die Möglichkeit, E-Mails mithilfe von Pretty Good Privacy (PGP) bzw. mithilfe des freien GNU Privacy Guards (GPG) zu verschlüsseln. Zeigen Sie, dass Sie E-Mail- Verschlüsselung beherrschen und schicken Sie eine mit PGP/GPG verschlüsselte Mail an `eik.list(at)uni-weimar.de` so dass wir diese auch wieder entschlüsseln können. Der Betreff sollte `[Krypto SS18] Beleg 1` sein. Im Klartext sollten Ihr(e) Name(n), Ihre Matrikelnummer(n) und der folgende Text stehen:

```
Es ist nicht genug zu wissen - man muss auch anwenden.
Es ist nicht genug zu wollen - man muss auch tun.
-- Johann Wolfgang v. Goethe
```

Hinweise:

- Für Thunderbird/icedove finden Sie Hinweise zur Installation und Benutzung des Addons `Enigmail` z.B. unter `http://www.thunderbird-mail.de/wiki/Enigmail_OpenPGP` Beachten Sie: `Enigmail` ist nur ein Addon. Sie benötigen noch `GPG`.

- Öffentliche Schlüssel lädt man auf einen vertrauenswürdigen Server hoch (nicht notwendig für diese Aufgabe). Die Standardadressen sind `pool.sks-keyservers.net`, `subkeys.pgp.net`, `sks.mit.edu`, `ldap://certserver.pgp.com`. Auf diesen finden Sie auch die öffentlichen Schlüssel der Professur.