Institut für Informatik
Prof. Dr. J. Rothe

Wintersemester 2023/24
Übungsblatt 5

Lösungsvorschläge

Kryptokomplexität 1

Bearbeitungszeit: 7. November bis 15-17. November
Verantwortlich: Roman Zorn

Aufgabe 1 : Tripel-Verschlüsselung

(a) Betrachten Sie die Verschiebungs-Chiffre aus der Vorlesung in Kombination mit der Tripel-Verschlüsselung und den Schlüsseln $k_1 = 7$, $k_2 = 2$ und $k_3 = 6$ über $\mathbb{Z}_{26}$.
► Verschlüsseln Sie den Klartext (inklusive Angabe Ihrer Rechenschritte)

$$m = \texttt{FISCHKUTTER}.$$

Lösungsvorschlag: ► Wir verschlüsseln zunächst mit k_3, entschlüsseln dann mit k_2 und verschlüsseln nochmals mit k_1. Es gilt

$$\texttt{FISCHKUTTER} \mathrel{\widehat{=}} (5\ 8\ 18\ 2\ 7\ 10\ 20\ 19\ 19\ 4\ 17).$$

Verschlüsseln mit $k_3 = 6$ ergibt (11 14 24 8 13 16 0 25 25 10 23), entschlüsseln mit $k_2 = 2$ ergibt (9 12 22 6 11 14 24 23 23 8 21) und verschlüsseln mit $k_1 = 7$ ergibt (16 19 3 13 18 21 5 4 4 15 2). Der Ciphertext ist also $c = \texttt{QTDNSVFEEPC}$.

(b) Betrachten Sie die Permutationschiffre in Kombination mit der Tripel-Verschlüsselung und den Schlüsseln $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$, $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$ und $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$.
► Entschlüsseln Sie den Ciphertext (inklusive Angabe Ihrer Rechenschritte)

$$c = \texttt{BERIFSSA}.$$

Lösungsvorschlag: ► Wir entschlüsseln zunächst mit ${\pi_1}^{-1}$, verschlüsseln dann mit π_2 und entschlüsseln nochmals mit ${\pi_3}^{-1}$. Wir zerteilen dazu c in zwei Blöcke der Länge 4. Es gilt

$$\pi_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \text{ und } \pi_3^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

Entschlüsseln mit ${\pi_1}^{-1}$ ergibt `ERIB` und `SSAF`, Verschlüsseln mit π_2 ergibt `IRBE` und `ASFS` und Entschlüsseln mit ${\pi_3}^{-1}$ ergibt `BIER` und `FASS`. Der Klartext ist also $m = \texttt{BIERFASS}$.

(c) ▶ Erhöht die Tripel-Verschlüsselung in Kombination mit der Verschiebungs- bzw. Permutationschiffre signifikant die Sicherheit des Kryptosystems? Begründen Sie Ihre Antwort.

Lösungsvorschlag: ▶ Nein, für beide Fälle lässt sich ein Schlüssel angeben, mit dessen Hilfe die Ver- bzw. Entschlüsselung in einem einzigen Schritt durchzuführen ist (in (a) und (b) wären das z.B. $k = 11$, bzw. $\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$). Der Aufwand, das Kryptosystem mit Tripel-Verschlüsselung zu knacken ist also der gleiche wie für das zugrundeliegende Kryptosystem.

Aufgabe 2 : Primfaktorzerlegung

▶ Zeigen Sie, dass jede natürliche Zahl $n \geq 2$ als Produkt von Primzahlen (und einer beliebigen Anzahl von Einsen) geschrieben werden kann.

Lösungsvorschlag: Wir zeigen per vollständiger Induktion, dass jede natürliche Zahl $n \geq 2$ als Produkt von Primzahlen (und einer beliebigen Anzahl von Einsen) geschrieben werden kann.

Induktionsanfang: Sei $n = 2$. 2 ist eine Primzahl und kann demnach als $2 \cdot 1$ geschrieben werden.

Induktionsannahme: Wir nehmen an, dass die Aussage für alle natürlichen Zahlen $2, \ldots, n-1$ gilt.

Induktionsschritt: $(n-1) \rightsquigarrow n$ Zeige die Aussage für n.

- Fall 1: n ist eine Primzahl. Dann kann n also als $n \cdot 1$ geschrieben werden. Zusammen mit der Induktionsannahme können die Zahlen $2, \ldots, n$ als Produkt von Primzahlen (und einer beliebigen Anzahl von Einsen) geschrieben werden.
- Fall 2: n ist keine Primzahl. Demnach existieren $x, y \in \mathbb{N} \setminus \{1\}$ mit $n = x \cdot y$. Es gilt $1 < x, y \leq n-1$. Nach der Induktionsannahme können x und y als Produkt von Primzahlen und Einsen geschrieben werden, also kann auch n als Produkt von Primzahlen und Einsen geschrieben werden und somit wieder alle Zahlen $2, \ldots, n$.

Aufgabe 3 : Euler Funktion

Sei φ die Euler Funktion, also $\varphi(n) = ||\mathbb{Z}_n^*||$ für eine natürliche Zahl $n \geq 1$.

(a) ► Zeigen Sie für jede Primzahl p und positive Zahl $k \in \mathbb{N}$, dass

$$\varphi(p^k) = p^k \cdot (1 - \frac{1}{p}).$$

Lösungsvorschlag: ► Sei p eine Primzahl und $k \in \mathbb{N}$. Es gilt $||\mathbb{Z}_{p^k}|| = p^k$. Da p eine Primzahl ist, wird p^k nur von 1 und p^i für $1 \leq i \leq k$ geteilt. Der ggT von p^k und einer natürlichen Zahl $n \leq p^k$ ist also genau dann ungleich 1, wenn n den Primfaktor p hat.

Also gilt $||\{i \in \mathbb{Z}_{p^k} \mid \text{ggT}(i, p^k) \neq 1\}|| = ||\{j \cdot p \mid 1 \leq j \leq p^{k-1}\}|| = p^{k-1}$.

Dann gilt $\varphi(p^k) = ||\mathbb{Z}_{p^k}^*|| = ||\{i \in \mathbb{Z}_{p^k} \mid \text{ggT}(i, p^k) = 1\}|| = ||\mathbb{Z}_{p^k}|| - ||\{i \in \mathbb{Z}_{p^k} \mid \text{ggT}(i, p^k) \neq 1\}|| = p^k - p^{k-1} = p^k(1 - p^{-1}) = p^k(1 - \frac{1}{p})$.

(b) ► Zeigen Sie, dass für jede natürliche Zahl $n \geq 2$ gilt, dass $\varphi(n) = n \prod_p (1 - \frac{1}{p})$, wobei p die Primfaktoren von n sind.

Hinweis: Nutzen Sie die Aussage aus Aufgabe 2 (beachten Sie, dass in der Primfaktorzerlegung manche Faktoren auch mehrfach vorkommen können) und Aufgabenteil (a).

Lösungsvorschlag: ► Sei $n \geq 2$ eine natürliche Zahl und $p_1, \ldots, p_\ell$ die Primfaktoren von n. Dann gibt es positive $k_1, \ldots, k_\ell \in \mathbb{N}$, sodass $n = \prod_{i=1}^{\ell} p_i^{k_i}$. Außerdem, da $p_i^{k_i}$ und $p_j^{k_j}$ für $i \neq j$ teilerfremd sind, gilt laut Vorlesung Kapitel 4, Seite 5, dass $\varphi(\prod_{i=1}^{\ell} p_i^{k_i}) = \prod_{i=1}^{\ell} \varphi(p_i^{k_i})$. Also gilt $\varphi(n) = \varphi(\prod_{i=1}^{\ell} p_i^{k_i}) = \prod_{i=1}^{\ell} \varphi(p_i^{k_i}) = \prod_{i=1}^{\ell} p_i^{k_i}(1 - \frac{1}{p_i}) = \prod_{i=1}^{\ell} p_i^{k_i} \cdot \prod_{i=1}^{\ell}(1 - \frac{1}{p_i}) = n \prod_{i=1}^{\ell}(1 - \frac{1}{p_i})$.

Aufgabe 4 : Ordnung von Gruppenelementen

Betrachten Sie, für eine Primzahl p, die Gruppe $(\mathbb{Z}_p^*, \cdot)$ aus der Vorlesung und sei $a \in \mathbb{Z}_p^*$.

(a) ▶ Zeigen Sie, dass für jedes $i, j \in \mathbb{Z}$ mit $j > i \geq 0$

$$a^i \equiv a^j \mod p \implies \text{ord}(a) \leq j - i$$

gilt, wobei wir mit $\text{ord}(a)$ die Ordnung von a in $\mathbb{Z}_p^*$ bezeichnen.

Lösungsvorschlag: ▶ Angenommen, es gilt $a^i \equiv a^j \mod p$ für beliebige $i, j \in \mathbb{Z}$ mit $j > i \geq 0$. Dann gilt für $k = j - i > 0$

$$a^k = a^{j-i} = a^j \cdot a^{-i} = a^j \cdot (a^i)^{-1} \equiv a^j \cdot (a^j)^{-1} \equiv 1 \mod p. \tag{1}$$

Somit muss die Ordnung von a kleiner oder gleich $k = j - i$ sein.

(b) ▶ Folgern Sie aus Aufgabeteil (a), dass nun alle $a^0, a^1, \ldots, a^{\text{ord}(a)-1}$ paarweise verschieden sein müssen.

Lösungsvorschlag: ▶ Angenommen, es wäre $a^i \equiv a^j \mod p$ für $0 \leq i < j < \text{ord}(a)$, dann wäre auch $\text{ord}(a) \leq j - i \leq j$ nach (1), was ein Widerspruch ist.

(c) ▶ Gelten die Aussagen aus Aufgabenteil (a) und (b) auch für eine beliebige positive Zahl $p \in \mathbb{N}$?

Lösungsvorschlag: ▶ Ja, denn wir haben an keiner Stelle unserer Beweise genutzt, dass p eine Primzahl sein muss. Somit gelten die Aussagen auch bei beliebigem $n \in \mathbb{N}_+$ für die Gruppe $(\mathbb{Z}_n^*, \cdot)$, $a \in \mathbb{Z}_n^*$ und unter der Annahme, dass $\text{ord}(a)$ die Ordnung von a in $\mathbb{Z}_n^*$ angibt.