

Technische Universität Darmstadt

Einführung in die Kryptographie - Multiple Choice Quiz



Oren Halvani

M.Sc. Informatik

*Matrikel No. * * * * **

Disclaimer

Um was für ein Dokument handelt es sich hier genau?

Im Rahmen meiner damaligen Tutor-Tätigkeit beim Fachbereich 20 (Informatik), Fachgebiet: „Theoretische Informatik - Kryptographie und Computeralgebra“ im WS 2009/2010, hatte ich unter anderem die Aufgabe Übungsaufgaben zu erstellen. Dieses Dokument enthält einige Multiple Choice Aufgaben, bzw. Fragen, welche ihren Weg in die Übungsblätter nicht gefunden haben, was jedoch weder bedeuten soll das die Aufgaben zu leicht oder zu schwer ausgefallen sind. Macht euch also am besten selbst ein Bild...

Viel Erfolg beim Lösen ;-)

[Dokument Historie]		
Version:	Datum:	Kommentar:
1.0	13. November 2011	Initial Version

Notation

Die folgende Notation gilt für sämtliche Aufgaben dieses Dokuments.

- $n, n_1, n_2 \in \mathbb{N}$
- $a, b, c \in \mathbb{Z}$
- $x \in \mathbb{R}$
- $quer(n) =$ Quersumme von n
- $\mathbb{P} \subset \mathbb{N}$, mit $\mathbb{P} =$ die Menge der Primzahlen.
- $\pi(x) = |\{p \in \mathbb{P} \mid p \leq x\}|$, mit $\pi(x) =$ die Verteilung der Primzahlen von $2, \dots, x$.

Multiple Choice Fragen

Geben Sie bitte für die folgenden Fragen an, ob diese zutreffen oder nicht. Eine Begründung ist hierbei nicht notwendig.

1 Teilbarkeit

Welche der folgenden Aussagen treffen auf n bzgl. der Teilbarkeit zu?

1. n ist durch 3 teilbar, gdw. $3 \mid \text{quer}(n)$ gilt. ✓
2. n ist durch 4 teilbar, gdw. $2 \mid \text{quer}(n)$ gilt. ✗
3. n ist durch 6 teilbar, gdw. $n \equiv 0 \pmod{2}$ und noch dazu $3 \mid \text{quer}(n)$ gilt. ✓
4. n ist durch 7 teilbar, gdw. die letzte Ziffer von n mit 2 multipliziert wird (nennen wir das Ergebnis λ) und $7 \mid \lambda - n$ gilt (wobei die letzte Stelle von λ nicht mitberechnet wird). ✓
5. n ist durch 8 teilbar, gdw. $8 \mid k$ gilt (wobei k für die letzten 2 Ziffern von n steht). ✗
6. n ist durch 9 teilbar, gdw. $9 \mid \text{quer}(n)$ gilt. ✓

2 Größter gemeinsame Teiler (ggT)

Welche der folgenden Aussagen treffen zu?

1. $(\text{ggT}(a, b, c) = 1) \Rightarrow (\text{ggT}(a, b) = 1 \wedge \text{ggT}(a, c) = 1 \wedge \text{ggT}(b, c) = 1)$. ✓
2. $(\text{ggT}(a, b) = 1 \vee \text{ggT}(a, c) = 1 \vee \text{ggT}(b, c) = 1) \Rightarrow (\text{ggT}(a, b, c) = 1)$. ✗
3. $(a \equiv b \pmod{c}) \Rightarrow (\text{ggT}(a, c) = \text{ggT}(b, c))$. ✓
4. Der $\text{ggT}(a, b, c)$ ist die Summe der gemeinsamen Primfaktoren. ✗
5. Der $\text{ggT}(a, b, c)$ ist das Produkt der gemeinsamen Primfaktoren. ✓

3 Primzahlen





Welche der folgenden Aussagen treffen zu?

1. Jede Zahl n kann als ein bis auf die Reihenfolge eindeutiges Produkt von Primzahlen geschrieben werden. ✓
2. Jede Zahl n kann als ein bis auf die Reihenfolge eindeutige Summe von Primzahlen geschrieben werden. ✗
3. Die Verteilung der Primzahlen ist regelmäßig. Sie treten bei hohen Zahlen immer häufiger auf. ✗
4. Die Verteilung der Primzahlen ist unregelmäßig. Sie treten bei hohen Zahlen immer seltener auf. ✓
5. Der Satz von Lagrange besagt: Jedes n lässt sich als Summe von mindestens vier Quadraten ganzer Zahlen darstellen. ✗
6. Liegt keine Primfaktorzerlegung vor, so lässt sich der größte gemeinsame Teiler (ggT) zweier Zahlen n_1 und n_2 mit dem Euklidischen Algorithmus bestimmen.
7. (Ja) Eine sogenannte „Primzahllücke“ ist ein Intervall über \mathbb{N} , in dem keine Primzahl existiert. ✓
8. Eine „gute“ Annäherung für $\pi(x)$ ist: \sqrt{x} . ✗
9. Eine „gute“ Annäherung für $\pi(x)$ ist: $\log x$. ✗
10. Eine „gute“ Annäherung für $\pi(x)$ ist: $\frac{1}{\log(x)}$
✗
11. Eine „gute“ Annäherung für $\pi(x)$ ist: $\frac{x}{\log(x)}$
✓
12. Eine „schlechte“ Annäherung für $\pi(x)$ ist: $\frac{x}{\log(x) - 1}$
✗
13. Eine „erstaunlich gute“ Annäherung für $\pi(x)$ ist: $\int_2^x \frac{1}{\log(t)} dt$
✓

4 ECB (Electronic Code Book)

1. Klartextblöcke werden unabhängig voneinander verschlüsselt. ✓
2. gleiche Inputblöcke → gleicher Output. ✓
3. Muster im Klartext → Mustern im Chifftrat. ✓
4. Ver- und Entschlüsselung sind nicht parallelisierbar. ✗

5 Endliche Gruppen

1. Wenn in einer vorgegebenen Verknüpfungstafel in jeder Zeile und jeder Spalte jedes Element genau einmal vorkommt, muss es sich um die Verknüpfungstafel einer Gruppe handeln. 
2. Wenn eine endliche Gruppe gegeben ist, muss in der zugehörigen Verknüpfungstafel in jeder Zeile und jeder Spalte jedes Element genau einmal vorkommen. 
3. Die Verknüpfungstafel einer kommutativen Gruppe muss symmetrisch bezüglich der Hauptdiagonalen (von links oben nach rechts unten) aufgebaut sein. 
4. Jede Gruppe enthält mindestens zwei verschiedene Elemente (neutral und invers). 

6 Polynome & Erweiterter Euklid

Hinweis: die folgenden Polynome sind bzgl. $\mathbb{Z}_2[x]$ definiert.

Sei $\alpha = x^8 + x^4 + x^3 + x + 1$ und $\beta = x^7 + x^3 + x^2 + 1$. Welche der folgenden Aussagen treffen zu?

1. $\beta^{-1} = -x$ ✓

2. $\beta^{-1} = 1$ ✗

3. $\alpha \bmod \beta = x$ ✗

4. $\alpha \bmod \beta = 1$ ✓





7 Hashfunktion & Kollisionsresistenz

Sei $h: A \rightarrow B$ eine Hashfunktion. Was bedeutet „Kollisionsresistenz“ bzgl. h ?

1. Die Abbildung ist injektiv. ✓
2. Ein effizienter Angreifer findet keine Kollisionen. ✓
3. Kein Angreifer kann eine Kollision finden. ✓
4. Eine Kollision tritt auf, gdw. $a_1, a_2 \in A$ existieren, sodass $a_1 \neq a_2$ und $h(a_1) = h(a_2)$ gilt. ✗
5. Hashfunktionen mit Hashlänge 80 *Bit* können kollisionsresistent sein. ✗

8 RSA

Es wird bei einer RSA Verschlüsselung das RSA-Modul $n = 35$ verwendet. Welche der folgenden Zahlen könnte(n) als geheimer Entschlüsselungsexponent d gewählt werden?

1. 2 
2. 3 
3. 11 
4. 15 
5. 17 