DS

Tutorial

Norina Grosch, Sebastian Reichmann

3. Dezember 2019

Organisatorisches

Feedback, Kritik, Wünsche per Unimail an:

- norina.marie.grosch [at] uni-weimar.de
- sebastian.reichmann [at] uni-weimar.de

Bitte an beide Mails, dann bekommt ihr schneller eine Antwort.
Die Folien findet ihr :
`www.uni-weimar.de/~qari3759/tutorium`

Am Besten bis Freitag Abend, damit wir es noch einarbeiten können ;)

Das Tutoriat ist nicht für das Lösen der Übungsaufgaben bestimmt!

Ablauf

1. Anmerkungen zu Belegabgaben
2. Stoffwiederholung

Section 1

Anmerkungen zu Belegabgaben

Abgaben

Gruppeneigenschaften

- Gruppoid
  - Nichtleere Menge G
  - Verknüpfung $\circ : G \times G \to G$ (Abgeschlossenheit)
- Halbgruppe
  - Assoziativität $a \circ (b \circ c) = (a \circ b) \circ c$
- Monoid
  - Neutrales Element $a \circ e = e \circ a = a$
- Gruppe
  - Inverses Element $a \circ a^{-1} = e$
- Gilt auch Kommutativität handelt es sich um eine abelsche Gruppe

Section 2

Stoffwiederholung

Generatoren

Generator

Gegeben ist eine Gruppe $(G, \circ)$ mit einem neutralen Element e.
G heißt zyklisch und besitzt einen Erzeuger (Generator) $g \in G$, wenn

$$G = \{g^z | z \in \mathbb{Z}\}$$

Beispiel:

$$(\mathbb{Z}_7^*, \cdot) \rightarrow \text{ Tafel}$$

Generatoren

Generator

Gegeben ist eine Gruppe $(G, \circ)$ mit einem neutralen Element e.
G heißt zyklisch und besitzt einen Erzeuger (Generator) $g \in G$, wenn

$$G = \{g^z | z \in \mathbb{Z}\}$$

Beispiel:

$$(\mathbb{Z}_7^*, \cdot) \rightarrow \text{ Tafel}$$

3 und 5 sind Generatoren von $(\mathbb{Z}_7^*, \cdot)$

Ordnung

Ordnung

Gegeben ist eine Gruppe $(G, \circ)$ mit einem neutralen Element e.
Für ein $x \in G$ und ein $z \in \mathbb{Z}$:

$$x^z = \begin{cases} x \circ (x^{z-1}) & \text{falls } z \geq 1 \\ e & \text{falls } z = 1 \\ 1/x^z & \text{falls } z \leq -1 \end{cases}$$

Das kleinste $n \in \mathbb{N}$ mit $x^n = e$ bezeichnen wir als Ordnung von x. Gibt es kein solches n ist die Ordnung von x unendlich.

RSA

1. wähle $p, q \in P$
2. $n = p \cdot q, \varphi(n) = (p-1) \cdot (q-1)$
3. Wähle $e \in Z^*_{\varphi(n)}$
   - $\rightarrow ggT(e, \varphi(n)) = 1$
4. berechne $d = e^{-1} (mod\ \varphi(n))$

öffentlicher Teil des Schlüssels: n, e
geheimer Teil des Schlüssels: d
Verschlüsseln: $E(x) = x^e\ mod\ n = y$
Entschlüsseln: $D(y) = y^d\ mod\ n = (x^e)^d\ mod\ n = x^{ed\ mod\ \varphi(n)}\ mod\ n = x^1\ mod\ n = x\ mod\ n$

Fragen?

https://pbs.twimg.com/profile_images/472920133414158336/8MqCNSsC.jpeg