

Crypto Workshop

Asymmetrische Kryptographie

Christoph Egger
Dominik Paulus

14. Mai 2018



MATHEMATIK

- ▶ Public-Key-Kryptographie funktioniert mit Mathematischen Strukturen
 - ▶ Gruppen
 - ▶ Gitter
 - ▶ ...
- ▶ Hier: Nur Gruppen, nur die Basics



GRUPPEN

Gruppen sind mathematische Strukturen (\mathbb{G}, \circ) .

- ▶ \mathbb{G} : Menge von Elementen

- ▶ \circ : "innere Verknüpfung"

Wenn $x \in \mathbb{G}$ und $y \in \mathbb{G}$ sind, dann ist auch $x \circ y \in \mathbb{G}$



GRUPPEN

Gruppen sind mathematische Strukturen (\mathbb{G}, \circ) .

- ▶ \mathbb{G} : Menge von Elementen

- ▶ \circ : "innere Verknüpfung"

Wenn $x \in \mathbb{G}$ und $y \in \mathbb{G}$ sind, dann ist auch $x \circ y \in \mathbb{G}$

Eigenschaften:

- ▶ Assoziativität: $a \circ (b \circ c) = (a \circ b) \circ c$

- ▶ Neutrales Element: e

Für $x \in \mathbb{G}$ ist $x \circ e = x = e \circ x$

- ▶ Für jedes Element gibt es ein Inverses: x^{-1}

$x \circ x^{-1} = e$



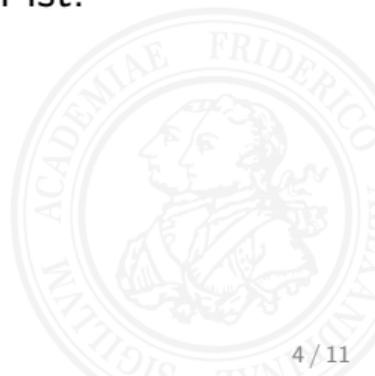
RESTKLASSENRINGE UND PRIMKÖRPER

- ▶ Ring: $(\mathbb{G}, +, \cdot)$, wobei (u. a.) $(\mathbb{G}, +)$ Gruppe ist.
- ▶ Restklassenringe $(\mathbb{Z}/n\mathbb{Z})$ sind eigentlich nur “Modulorechnen” modulo n
- ▶ Wichtig: Fast alles, was man von ganzen Zahlen kennt geht immer noch!



RESTKLASSENRINGE UND PRIMKÖRPER

- ▶ Ring: $(\mathbb{G}, +, \cdot)$, wobei (u. a.) $(\mathbb{G}, +)$ Gruppe ist.
- ▶ Restklassenringe $(\mathbb{Z}/n\mathbb{Z})$ sind eigentlich nur “Modulorechnen” modulo n
- ▶ Wichtig: Fast alles, was man von ganzen Zahlen kennt geht immer noch!
- ▶ Primkörper \mathbb{F}_p sind Restklassenringe, bei denen n eine Primzahl ist.
- ▶ Mehr Details und Eigenschaften: \rightarrow Mathevorlesung



ZYKLISCHE UNTERGRUPPEN

- ▶ In unserem Primkörper \mathbb{F}_p gibt es (multiplikative) Untergruppen, die entstehen wenn man ein einzelnes Element auswählt und immer wieder mit sich selbst verknüpft



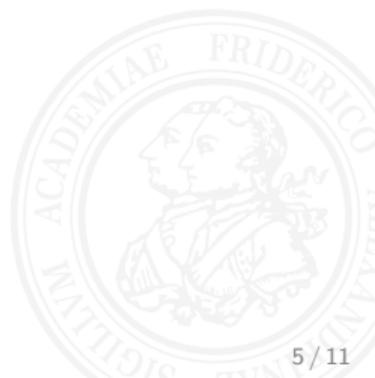
ZYKLISCHE UNTERGRUPPEN

- ▶ In unserem Primkörper \mathbb{F}_p gibt es (multiplikative) Untergruppen, die entstehen wenn man ein einzelnes Element auswählt und immer wieder mit sich selbst verknüpft
- ▶ Wähle \mathbb{F}_7 : $\langle 2 \rangle = \{2, 2^2, 2^3, \dots\} = \{2, 4, 1\}$



ZYKLISCHE UNTERGRUPPEN

- ▶ In unserem Primkörper \mathbb{F}_p gibt es (multiplikative) Untergruppen, die entstehen wenn man ein einzelnes Element auswählt und immer wieder mit sich selbst verknüpft
- ▶ Wähle \mathbb{F}_7 : $\langle 2 \rangle = \{2, 2^2, 2^3, \dots\} = \{2, 4, 1\}$
- ▶ Es gibt auch degenerierte Fälle:
 $\langle 1 \rangle = \{1, 1^2, 1^3, \dots\} = \{1\}$
 $\langle -1 \rangle = \{-1, (-1)^2, (-1)^3, \dots\} = \{-1, 1\}$



DLOG ET. AL.

Reelle Zahlen:

$$x = y^z$$

$$z = \log_y x$$

“einfach”

Primkörper:

$$x \equiv y^z \pmod{n}$$

$$z = f(x, y, n)$$

“schwer”



DH KEY-EXCHANGE

Diffie-Hellman Key-Exchange

$$x \leftarrow_{\$} \{0, 1\}^{\lambda}$$

$$y \leftarrow_{\$} \{0, 1\}^{\lambda}$$

$$g^x$$



$$g^y$$



$$\text{return}(g^y)^x$$

$$\text{return}(g^x)^y$$



FRAGEN?

42



SIMPLE SERVER

- ▶ Hier wurde nichts “gehackt” sondern nur das Protokol implementiert!
- ▶ Die Parameter waren auch schon vernünftig gewählt – `openssl dhparam`



SMALL GROUPS

- ▶ Client (ihr!) hat nicht mehr genug Informationen für den Schlüsselaustausch



SMALL GROUPS

- ▶ Client (ihr!) hat nicht mehr genug Informationen für den Schlüsselaustausch
- ▶ Der Client kann aber einen (auch einen unsicheren) Generator wählen
- ▶ Die trivialen Fälle 0 und 1 sind aber ausgeschlossen



SMALL GROUPS

- ▶ Client (ihr!) hat nicht mehr genug Informationen für den Schlüsselaustausch
- ▶ Der Client kann aber einen (auch einen unsicheren) Generator wählen
- ▶ Die trivialen Fälle 0 und 1 sind aber ausgeschlossen
- ▶ Es verbleiben aber noch genug unsichere Generatoren. Im besonderen ist $|\langle -1 \rangle| = 2$, d. h. es gibt nur 2 mögliche keys mit diesem Generator
- ▶ Einfach beide probieren, mit einem davon kann man die Daten dann entschlüsseln



FRAGEN?

42

