

## Lösungsvorschläge Kryptokomplexität II

Bearbeitungszeit: 7. Mai bis 17. Mai  
Verantwortlich: Roman Zorn

### Aufgabe 1: Algorithmus von Pohlig und Hellman

► Berechnen Sie  $a = \log_2 26$  in  $\mathbb{Z}_{37}^*$  mit dem Algorithmus von Pohlig und Hellman.

**Lösungsvorschlag:**  $\gamma = 2$  ist ein primitives Element für  $\mathbb{Z}_{37}^*$ , da  $2^{18} \equiv 36 \pmod{37}$  und  $2^{12} \equiv 26 \pmod{37}$  gilt, vgl. Blatt 03. Mit den Werten  $n = 36 = 2^2 \cdot 3^2$ ,  $\alpha = 26$  und  $\gamma = 2$  berechnen wir:

(i)  $q_1 = 2$ ,  $c_1 = 2$ ,

$j = 0$ : Es gilt  $\alpha_0 = 26$  und  $\delta = \alpha_0^{n/q_1^1} = 26^{18} \equiv 1 \pmod{37}$ . Für  $i$  ergibt sich dann aus  $\gamma^{0 \cdot n/q_1} = 2^{0 \cdot 18} = 1 = \delta$  der Wert  $i = 0$ , so dass  $a_0 = 0$  folgt. Im letzten Schritt ergibt sich  $\alpha_1 = \alpha_0 \cdot \gamma^{-a_0 q_1^0} = 26 \cdot 2^{0 \cdot 1} \equiv 26 \pmod{37}$ .

$j = 1$ :  $\alpha_1 = 26$ ,  $\delta = \alpha_1^{n/q_1^2} = 26^9 \equiv 1 \pmod{37}$ ,  $\gamma^{0 \cdot n/q_1} = 2^{0 \cdot 18} = 1 = \delta$ ,  
 $\implies i = 0$ ,  $\implies a_1 = 0$ ,  
 $\alpha_2 = \alpha_1 \cdot \gamma^{-a_1 q_1^1} = 26 \cdot 2^{0 \cdot 2} \equiv 26 \pmod{37}$ .

Wir erhalten  $a = 0 \cdot 2^0 + 0 \cdot 2^1 \equiv 0 \pmod{2^2}$ .

(ii)  $q_2 = 3$ ,  $c_2 = 2$ ,

$j = 0$ :  $\alpha_0 = 26$ ,  $\delta = \alpha_0^{n/q_2^1} = 26^{12} \equiv 1 \pmod{37}$ ,  $\gamma^{0 \cdot n/q_2} = 2^{0 \cdot 12} = 1 = \delta$ ,  
 $\implies i = 0$ ,  $\implies a_0 = 0$ ,  
 $\alpha_1 = \alpha_0 \cdot \gamma^{-a_0 q_2^0} = 26 \cdot 2^{0 \cdot 1} \equiv 26 \pmod{37}$ .

$j = 1$ :  $\delta = \alpha_1^{n/q_2^2} = 26^4 \equiv 26 \pmod{37}$ ,  $\gamma^{1 \cdot n/q_2} = 2^{1 \cdot 12} \equiv 26 \pmod{37}$ ,  
 $\implies i = 1$ ,  $\implies a_1 = 1$ ,  
 $\alpha_2 = \alpha_1 \cdot \gamma^{-a_1 q_2^1} = 26 \cdot 2^{1 \cdot 3} \equiv 31 \pmod{37}$ .

Wir erhalten  $a \equiv 0 \cdot 3^0 + 1 \cdot 3^1 \equiv 3 \pmod{9}$ .

Mit dem Chinesischen Restsatz lässt sich das Kongruenzsystem

$$\begin{aligned} a &\equiv 0 \pmod{4}, \\ a &\equiv 3 \pmod{9}, \end{aligned}$$

wie folgt lösen:  $M = 4 \cdot 9 = 36$ ,  $q_1 = 9$ ,  $q_2 = 4$  sowie  $1 \cdot 9 - 2 \cdot 4 = 1$ , also

$$q_1^{-1} \equiv 9^{-1} \equiv 1 \pmod{4}, \quad q_2^{-1} \equiv 4^{-1} \equiv 7 \pmod{9}.$$

Insgesamt ist die gesuchte Lösung modulo 36 gegeben durch

$$0 \cdot 9 \cdot 1 + 4 \cdot 7 \cdot 3 \equiv 12 \pmod{36}.$$

Demnach gilt  $\log_2 26 = 12$  in  $\mathbb{Z}_{37}^*$ , d.h.  $2^{12} \equiv 26 \pmod{37}$ .

## Aufgabe 2: ElGamals Public-Key-Kryptosystem

- (a) Alice und Bob einigen sich auf  $p = 367$  und das primitive Element  $\gamma = 17$  in  $\mathbb{Z}_{367}^*$ . Alice möchte die Nachricht  $m = 103$  an Bob verschicken und wählt dafür die private Zahl  $a = 97$ . Bob wählt die private Zahl  $b = 129$ .
- Führen Sie das Protokoll für das Kryptosystem von ElGamal durch. Geben Sie dabei alle benötigten Zwischenschritte an.
- (b) Alice möchte die Nachrichten  $m_1$  und  $m_2$  verschlüsseln. Sie wählt bei beiden Verschlüsselungen die gleiche zufällige Zahl  $a$ .  $\alpha_{2,i}$  bezeichne für  $i \in \{1, 2\}$  das von Alice berechnete  $\alpha_2$  der  $i$ -ten Nachricht.
- Zeigen Sie, dass sich bei bekannter Nachricht  $m_2$  die Nachricht  $m_1$  durch die Gleichung  $m_1 = \alpha_{2,1} \cdot \alpha_{2,2}^{-1} \cdot m_2$  berechnen lässt.

## Lösungsvorschlag:

- (a) Wir haben  $p = 367$  und  $\varphi(367) = 366 = 2 \cdot 3 \cdot 61$ . Mit  $17^{187} \equiv 366 \pmod{367}$ ,  $17^{122} \equiv 283 \pmod{367}$ , und  $17^6 \equiv 346 \pmod{367}$  folgt, dass  $\gamma$  ein primitives Element in  $\mathbb{Z}_{367}^*$  ist.

Wir führen ElGamals Public-Keykryptosystem durch:

| Alice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Bob                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | $b = 129$<br>$\beta = \gamma^b = 17^{129}$<br>$\equiv 261 \pmod{367}$                                                   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | $\xleftarrow{\beta=261}$                                                                                                |
| $a = 97$<br>$m = 103$<br>$\alpha_1 = \gamma^a = 17^{97} \equiv 123 \pmod{367}$<br>$\alpha_2 = m\beta^a = 103 \cdot 261^{97}$<br>$\equiv 103 \cdot 203 \pmod{367}$<br>$\equiv 357 \pmod{367}$                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                         |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | $\xrightarrow{\alpha_1=123, \alpha_2=357}$                                                                              |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | $m = \alpha_2 \alpha_1^{-b}$<br>$= 357 \cdot 185^{129}$<br>$\equiv 357 \cdot 320 \pmod{367}$<br>$\equiv 103 \pmod{367}$ |
| (b) Es gilt                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                         |
| $ \begin{aligned} \alpha_{2,1} \cdot \alpha_{2,2}^{-1} &\equiv \alpha_{2,1} \cdot \alpha_{2,2}^{p-2} \pmod{p} \\ &\equiv m_1 \cdot \beta^a \cdot (m_2 \cdot \beta^a)^{p-2} \pmod{p} \\ &\equiv m_1 \cdot \beta^a \cdot m_2^{p-2} \cdot \beta^{a(p-2)} \pmod{p} \\ &\equiv m_1 \cdot m_2^{p-2} \cdot \beta^{a+ap-2a} \pmod{p} \\ &\equiv m_1 \cdot m_2^{p-2} \cdot \beta^{a(p-1)} \pmod{p} \\ &\equiv m_1 \cdot m_2^{p-2} \cdot (\beta^{p-1})^a \pmod{p} \\ &\equiv m_1 \cdot m_2^{p-2} \cdot 1^a \pmod{p} \\ &\equiv m_1 \cdot m_2^{p-2} \pmod{p}. \end{aligned} $ |                                                                                                                         |
| Die Gleichung $\alpha_{2,1} \cdot \alpha_{2,2}^{-1} \equiv m_1 \cdot m_2^{p-2} \pmod{p}$ kann man zu                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                         |
| $\alpha_{2,1} \cdot \alpha_{2,2}^{-1} \cdot m_2 \equiv m_1 \cdot m_2^{p-2} \cdot m_2 \pmod{p}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                         |
| und somit (kleiner Fermat) zu $\alpha_{2,1} \cdot \alpha_{2,2}^{-1} \cdot m_2 \equiv m_1 \pmod{p}$ umformen.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                         |

### Aufgabe 3: ElGamal – Signaturen

Betrachten Sie das digitale Signatur-Schema von ElGamal mit den bekannten Werten  $p = 383$  und  $\gamma = 5$ .

- (a) ► Für die Signatur einer Nachricht muss Bob eine geheime Zahl  $s$  wählen. Begründen Sie, welche der folgenden  $s_i$  gültig sind.

- $s_1 = 1$
- $s_2 = 29$
- $s_3 = 38$

**Lösungsvorschlag:** Für  $s$  muss gelten  $\gcd(s, p-1) = \gcd(s, 382) = 1$ . Das wird nur von  $s_1 = 1$  und  $s_2 = 29$  erfüllt.

*Hinweis:* Die Wahl von  $s = 1$  ist aber nicht sinnvoll, da dann in der Signatur  $\sigma = \gamma^1 = \gamma$  gilt. Ein Angreifer, der eine Signatur mit  $\sigma = \gamma$  sieht, weiß so sofort, dass  $s = 1$  gewählt wurde. Wegen  $\rho = (m - b \cdot \sigma)s^{-1} \equiv m - b \cdot \gamma \pmod{p-1}$  folgt dann  $b \equiv -(\rho - m)\gamma^{-1} \pmod{p-1}$ . Da  $p, \rho, \gamma, m$  bekannt sind, könnte man dann den privaten Schlüssel  $b$  berechnen.

- (b) ► Bob wählt den privaten Exponenten  $b = 15$ . Signieren Sie die Nachricht  $m = 23$  mit  $s = 29$ .

**Lösungsvorschlag:**

- Zunächst berechnen wir  $\beta = \gamma^b = 5^{15} \equiv 245 \pmod{383}$ .
- Wir berechnen nun  $\sigma = \gamma^s \equiv 5^{29} \equiv 132 \pmod{383}$ .
- Wir lösen die Kongruenz  $b\sigma + s\rho \equiv m \pmod{p-1}$  nach  $\rho$  auf:

$$\begin{aligned} b\sigma + s\rho &\equiv m \pmod{p-1} \\ 15 \cdot 132 + 29\rho &\equiv 23 \pmod{382} \\ 29\rho &\equiv 23 - 15 \cdot 132 \pmod{382} \\ \rho &\equiv (23 - 15 \cdot 132) \cdot 303 \pmod{382} \quad (\text{weil } 29^{-1} \equiv 303 \pmod{382}) \\ \rho &\equiv 275 \pmod{382} \end{aligned}$$

Die Signatur ist nun  $\langle m, \beta, (\sigma, \rho) \rangle = \langle 23, 245, (132, 275) \rangle$ .

- (c) ► Ist folgende Signatur gültig bei  $p = 383$  und  $\gamma = 5$ ?

$$\langle 24, 25, (163, 69) \rangle$$

**Lösungsvorschlag:** Zum Verifizieren prüft man die Kongruenz

$$\begin{aligned} \gamma^m &\equiv \beta^\sigma \cdot \sigma^\rho \pmod{p} \\ 5^{24} &\equiv 25^{163} \cdot 163^{69} \pmod{383} \\ 21 &\equiv 373 \cdot 77 \pmod{383} \\ 21 &\not\equiv 379 \pmod{383} \quad \times \end{aligned}$$

Also ist die Signatur ungültig.

#### Aufgabe 4: ElGamal – Key-only-Angriff

Betrachten Sie erneut das digitale Signatur-Schema von ElGamal mit den bekannten Werten  $p = 383$ ,  $\gamma = 5$ . Diesmal ist  $\beta = 68$ .

- (a) ► Welche Nachricht  $m$  kann ein Angreifer signieren, wenn er für einen Key-only-Angriff die Zahlen  $x = 33$  und  $y = 7$  wählt? Geben Sie auch die Signatur an.

**Lösungsvorschlag:** Zunächst berechnet der Angreifer  $y^{-1} \bmod p - 1$  also  $7^{-1} \equiv 273 \bmod 382$ . Dann berechnet er  $\sigma, \rho$  und  $m$ :

$$\begin{aligned}\sigma &= \gamma^x \cdot \beta^y = 5^{33} \cdot 68^7 \equiv 155 \cdot 185 \equiv 333 && \bmod 383, \\ \rho &= -\sigma \cdot y^{-1} = -333 \cdot 273 \equiv -375 \equiv 7 && \bmod 382, \\ m &= -x \cdot \sigma \cdot y^{-1} \equiv -33 \cdot 333 \cdot 273 \equiv -151 \equiv 231 && \bmod 382.\end{aligned}$$

Also ist  $(\sigma, \rho) = (333, 7)$  eine gültige Signatur für  $m = 231$ . Der Angreifer sendet  $\langle m, \beta, (\sigma, \rho) \rangle = \langle 231, 68, (333, 7) \rangle$ .

*Bemerkung: Den privaten Exponenten  $b = 42$  weiß der Angreifer nicht, er ist aber wie oben gezeigt auch nicht nötig um die Signatur zu fälschen.*

- (b) ► Zeigen Sie, dass Ihre in (a) berechnete Signatur tatsächlich gültig ist.

**Lösungsvorschlag:** Wir erhalten die signierte Nachricht  $\langle 231, 68, (333, 7) \rangle$  und prüfen die folgende Kongruenz:

$$\begin{aligned}\gamma^m &\equiv \beta^\sigma \cdot \sigma^\rho && \bmod p \\ 5^{231} &\equiv 68^{333} \cdot 333^7 && \bmod 383 \\ 319 &\equiv 43 \cdot 239 && \bmod 383 \\ 319 &\equiv 319 && \bmod 383 \quad \checkmark\end{aligned}$$

- (c) ► Bewerten Sie, wie geeignet der Angriff ist, um gezielt eine bestimmte Nachricht in falschem Namen zu signieren.

**Lösungsvorschlag:** Der Angreifer muss unter Umständen eine große Anzahl an Werten für  $x$  und  $y$  ausprobieren, bis er eine Signatur zu einer Nachricht  $m$  erhält, die auch Sinn ergibt. Im Allgemeinen kommen vor allem unsinnige Nachrichten heraus und es ist bisher kein effizienter Weg bekannt,  $x$  und  $y$  so zu wählen, dass eine bestimmte Nachricht  $m$  signiert wird. Das macht den Angriff in der Praxis eher weniger relevant.