Lösungsvorschläge
Kryptokomplexität IIBearbeitungszeit: 30. April bis 10. Mai
Verantwortlich: Roman Zorn**Aufgabe 1:** Primitive Elemente IIIEs sei p eine ungerade Primzahl und γ ein primitives Element in $\mathbb{Z}_p^*$.

► Zeigen Sie:

$$\text{Es gilt } \gamma^{(p-1)/2} \equiv -1 \pmod{p}.$$

Lösungsvorschlag: Diese Aufgabe beruht auf der Arbeit von Wätjen [Wat08].Wir wissen, dass $p > 2$ eine Primzahl ist. Weiterhin ist γ ein primitives Element in $\mathbb{Z}_p^*$, also folgt nach Definition, dass für alle $1 \leq x < \varphi(p)$ gilt

$$\gamma^x \not\equiv 1 \pmod{p}. \quad (1)$$

Insbesondere gilt diese Aussage auch für $\frac{p-1}{2} < p-1 = \varphi(p)$. Weiterhin gilt

$$(\gamma^{(p-1)/2})^2 \equiv \gamma^{(p-1)/2 \cdot 2} \equiv \gamma^{p-1} \stackrel{\text{kl.Fmt.}}{\equiv} 1 \pmod{p}.$$

Die einzigen Elemente in $\mathbb{Z}_p^*$, die quadriert 1 liefern, sind 1 und -1. Das bedeutet, dass

$$\gamma^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

gelten muss, da die andere Möglichkeit bereits durch (1) ausgeschlossen wurde.

Literatur[Wat08] D. Wätjen. *Kryptographie. Grundlagen, Algorithmen, Protokolle*. Spektrum Akademischer Verlag, 2008.**Aufgabe 2:** Schlüsselvereinbarung von Diffie und Hellman

- (a) ► Zeigen Sie, dass $\gamma = 17$ ein primitives Element in $\mathbb{Z}_{487}^*$ ist.
- (b) ► Führen Sie das Schlüsselvereinbarungsprotokoll von Diffie und Hellman für $p = 487$, $\gamma = 17$, $a = 112$ und $b = 72$ durch. Geben Sie dabei alle relevanten Zwischenschritte an.

Lösungsvorschlag:

- (a) Um zu zeigen, dass $\gamma = 17$ ein primitives Element in $\mathbb{Z}_{487}^*$ ist, gehen wir wie folgt vor. Im ersten Schritt sehen wir, dass $p = 487$ eine Primzahl ist. Damit können wir die Aussage aus der Vorlesung, dass ein Element $\kappa \in \mathbb{Z}_p^*$ genau dann ein primitives Element für $\mathbb{Z}_p^*$ ist, wenn $\kappa^{(p-1)/q} \not\equiv 1 \pmod p$ für alle Primzahlen q , die $p - 1$ teilen, gilt, nutzen. Es gilt

$$\varphi(p) = 486 = 2 \cdot 3^5.$$

Damit sind alle Primzahlen, die $p - 1 = \varphi(p)$ teilen, die Zahlen 2 und 3. Um also festzustellen ob $\gamma = 17$ ein primitives Element ist, müssen wir testen ob

$$17^{486/2} \not\equiv 1 \pmod{487} \quad \text{und} \\ 17^{486/3} \not\equiv 1 \pmod{487}$$

gilt. Mit Square-and-Multiply berechnen wir

$$17^{243} \equiv 486 \pmod{487} \quad \text{und} \\ 17^{162} \equiv 254 \pmod{487}$$

und können so folgern, dass 17 ein primitives Element von $\mathbb{Z}_{487}^*$ ist.

- (b) Die Werte $p = 487$, $\gamma = 17$, $a = 112$, und $b = 72$ sind bereits bekannt. Im nächsten Schritt berechnen wir die öffentlichen Werte α und β zu

$$\alpha = \gamma^a = 17^{112} \equiv 196 \pmod{487} \quad \text{und} \\ \beta = \gamma^b = 17^{72} \equiv 60 \pmod{487}.$$

α und β werden nun öffentlich ausgetauscht. Anschließend können wir den privaten Schlüssel k_A bzw. k_B berechnen als

$$k_A = \beta^a = 60^{112} \equiv 443 \pmod{487} \quad \text{und} \\ k_b = \alpha^b = 196^{72} \equiv 443 \pmod{487}.$$

Aufgabe 3: Man-in-the-Middle-Angriff

Seien $p = 37$ und $\gamma = 18$ für eine Schlüsselvereinbarung nach dem Protokoll von Diffie und Hellman gegeben. Alice und Bob wählen die privaten Zahlen $a = 103$ bzw. $b = 97$. Allerdings fängt ein *Man in the Middle* die öffentlichen Zahlen α und β ab und führt mit der Zahl $e = 7$ einen *Man-in-the-Middle-Angriff* durch.

- (a) ► Welchen Schlüssel $k_{A,E}$ teilt er sich mit Alice und welchen Schlüssel $k_{B,E}$ teilt er sich mit Bob?
- (b) ► Welche Schlüssel $k_{E,A}$ und $k_{E,B}$ berechnet der *Man in the Middle*?
- (c) ► Welchen Schlüssel hätten sich Alice und Bob ohne den Angriff geteilt?

Lösungsvorschlag: $p = 37$ ist eine Primzahl. Mit $\varphi(37) = 36 = 2^2 \cdot 3^2$ folgt schnell, dass $\gamma = 18$ ein primitives Element in $\mathbb{Z}_{37}^*$ ist, da $18^{18} \equiv 36 \pmod{37}$ und $18^{12} \equiv 10 \pmod{37}$ gilt, vgl. Blatt 03. Wir können das Schlüsselvereinbarungsprotokoll von Diffie und Hellman also anwenden:

Schritt	Alice	Man in the Middle	Bob
1	$p = 37, \gamma = 18$		$p = 37, \gamma = 18$
2	$a = 103$		$b = 97$
3	$\alpha = 18^{103} \equiv 5 \pmod{37}$ $\xrightarrow{\alpha}$	$e = 7$ $\alpha_E, \beta_E = 18^7$ $\equiv 13 \pmod{37}$ $\xleftrightarrow{\beta_E \quad \alpha_E}$	$\beta = 18^{97} \equiv 24 \pmod{37}$ $\xleftarrow{\beta}$
4	$k_{A,E} = \beta_E^a = 13^{103}$ $\equiv 18 \pmod{37}$	$k_{E,A} = \alpha^e = 5^7$ $\equiv 18 \pmod{37}$ $k_{E,B} = \beta^e = 24^7$ $\equiv 5 \pmod{37}$	$k_{B,E} = \alpha_E^b = 13^{97}$ $\equiv 5 \pmod{37}$

- (a) Der *Man in the Middle* teilt sich mit Alice also den Schlüssel $k_{A,E} = 18$ und mit Bob den Schlüssel $k_{B,E} = 5$.
- (b) Der *Man in the Middle* berechnet die Schlüssel $k_{E,A} = 18$ und $k_{E,B} = 5$.
- (c) Ohne den Angriff wäre der Schlüssel

$$k_A = \beta^a = 24^{103} \equiv 19 \pmod{37} \equiv 5^{97} = \alpha^b = k_B$$

gewesen.

Aufgabe 4: Algorithmus von Shanks

- Berechnen Sie $a = \log_3 101$ in $\mathbb{Z}_{127}^*$ mit dem Algorithmus von Shanks.

Lösungsvorschlag: Für den Algorithmus von Shanks gilt aus der Aufgabenstellung $G = \mathbb{Z}_{127}^*$, also $n = \varphi(127) = 126 = 2 \cdot 3^2 \cdot 7$. Weiterhin stellen wir schnell fest, dass

$\gamma = 3$ ein primitives Element in $\mathbb{Z}_{127}^*$ ist, da

$$\begin{aligned} 3^{63} &\equiv 126 \pmod{127}, \\ 3^{42} &\equiv 107 \pmod{127} \quad \text{und} \\ 3^{18} &\equiv 4 \pmod{127} \end{aligned}$$

gilt. Für $\alpha = 101$ gilt weiter $s = \lceil \sqrt{126} \rceil = 12$. Wir berechnen nun für $0 \leq i \leq s - 1$ die Werte $\gamma^{i \cdot s}$:

i	0	1	2	3	4	5	6	7	8	9	10	11
$3^{i \cdot 12} \pmod{127}$	1	73	122	16	25	47	2	19	117	32	50	94

Aufsteigend nach $\gamma^{i \cdot s}$ sortiert erhalten wir

$$\begin{aligned} \mathcal{L}_1 = \{ &(1, 0), (2, 6), (16, 3), (19, 7), (25, 4), (32, 9), \\ &(47, 5), (50, 10), (73, 1), (94, 11), (117, 8), (122, 2) \}. \end{aligned}$$

Jetzt berechnen wir für $0 \leq j \leq s - 1$ die Werte $\alpha \gamma^{-j}$:

j	0	1	2	3	4	5	6	7	8	9	10	11
$101 \cdot 3^{-j} \pmod{127}$	101	76	110	79	111	37	97	117	39	13	89	72

Aufsteigend nach $\alpha \gamma^{-j}$ sortiert erhalten wir

$$\begin{aligned} \mathcal{L}_2 = \{ &(13, 9), (37, 5), (39, 8), (72, 11), (76, 1), (79, 3), \\ &(89, 10), (97, 6), (101, 0), (110, 2), (111, 4), (117, 7) \}. \end{aligned}$$

Wir suchen nun ein Paar $(\delta, i) \in \mathcal{L}_1$ und ein Paar $(\delta, j) \in \mathcal{L}_2$ mit gleichem ersten Eintrag. Das sind die Paare $(117, 8)$ und $(117, 7)$. Damit gilt:

$$\log_3(101) = i \cdot s + j = 8 \cdot 12 + 7 = 103 \pmod{127}.$$

Die entsprechende Rechnung lautet

$$\begin{aligned} 3^{8 \cdot 12} &\equiv 101 \cdot 3^{-7} \pmod{127} \\ \xrightarrow{\cdot 3^7} 3^{8 \cdot 12 + 7} &\equiv 101 \pmod{127} \\ \xrightarrow{\log_3} 8 \cdot 12 + 7 &\equiv \log_3 101 \pmod{127}. \end{aligned}$$