

Index-Calculus-Methode für diskrete Logarithmierung und das ElGamal-Kryptosystem

Aufgabe 1. Mit Hilfe der Index-Calculus-Methode finden Sie alle Lösungen der Kongruenz

$$7^x \equiv 100 \pmod{601}. \quad (1)$$

Dafür benutzen Sie folgende Kongruenzen:

$$\begin{aligned} 7^8 &\equiv 3^2 \pmod{601}, \\ 7^{24} &\equiv 2^7 \pmod{601}, \\ 7^{14} &\equiv 5 \cdot 3 \cdot 2^5 \pmod{601}. \end{aligned}$$

Aufgabe 2. Mit Hilfe des Pohlig-Hellman-Algorithmus finden Sie alle Lösungen der Kongruenz (1).

Aufgabe 3. Alice will die Zahlen aus der Gruppe \mathbb{Z}_{601}^* mit Hilfe des ElGamal-Kryptosystems chifrieren. Sie wählt einen privaten Schlüssel $a = 237$ und veröffentlicht den öffentlichen Schlüssel $(p, g, A) = (601, 7, 194)$.

a) Sei $x = 123$ ein Klartext, den Alice chifrieren will. Wie wird der Chiffretext aussehen, wenn ihr Computer $k = 57$ als zufälliges Parameter wählt?

b) Bob erhält einen Chiffretext $(2, 3)$ von Alice. Wie sieht der Klartext x aus?

Aufgabe 4. Alice will die Zahlen aus der Gruppe \mathbb{Z}_{601}^* mit Hilfe des ElGamal-Kryptosystems chifrieren. Ihre öffentlichen Schlüssel ist $(p, g, A) = (601, 7, 99)$. Welchen Wert hat ihr privater Schlüssel?