Kryptologie

Übung, LVA 405.321
C. Fuchs

9. Übungsblatt, SS 2022

18.05.2022

1. Angenommen Alice und Bob einigen sich auf das folgende Kryptosystem: Alice wählt $a, b \in \mathbb{Z}$ und berechnet $M = ab - 1$. Dann wählt Alice zwei ganze Zahlen a', b' und berechnet $e = a'M + a$ und $d = b'M + b$. Dann berechnet sie $n = (ed - 1)/M$. Das Paar (n, e) ist der öffentliche und die ganze Zahl d der geheime Schlüssel von Alice. Wenn Bob eine Nachricht $m \in \{0, 1, \ldots, n - 1\}$ an Alice senden möchte, berechnet er $c = em \bmod n$ und sendet c an Alice. Alice entschlüsselt die Nachricht mittels $cd \bmod n$. Zeige, dass es sich um ein (Public-Key-)Kryptosystem handelt. Wie kann das Kryptosystem für digitale Signaturen verwendet werden? Brich das Kryptosystem.

2. Das folgende Public-Key-Kryptosystem wurde von ElGamal vorgeschlagen. Alle Benutzer kennen dieselbe große Primzahl p und eine Primitivwurzel a modulo p. Alice wählt eine natürliche Zahl d zufällig als geheimen Schlüssel. Als öffentlichen Schlüssel gibt sie $e = a^d \bmod p$ bekannt. Wenn Bob eine Nachricht $m \in \{1, \ldots, p - 1\}$ an Alice senden möchte geht er folgendermaßen vor: 1) Er wählt zufällig eine Zahl k mit $1 \leq k \leq p-1$, 2) er berechnet $c = e^k \bmod p$, 3) er sendet das Paar $(c_1, c_2) = (a^k \bmod p, cm \bmod p)$ an Alice. Zeige, dass dieses System die Anforderungen eines Public-Key-Kryptosystems erfüllt.

3. Zeige, dass ein polynomialer Algorithmus zur Berechnung des diskreten Logarithmus das ElGamal-Kryptosystem brechen würde.

4. Wir nehmen im ElGamal-Kryptosystem $p = 71$ mit der Primitivwurzel 7. Angenommen für den öffentlichen Schlüssel von Benutzer A gilt $e = 3$ und Benutzer B wählt den Schlüssel $k = 2$. Wie sieht der Ciphertext zu $m = 30$ aus? Angenommen, unter Benutzung eines neuen Schlüssels k', wird $m = 30$ als $(2, c_2)$ gesandt. Was ist c_2?