

7. Übung Kryptographie

1. Aufgabe

Seien $(n_A, 3)$, $(n_B, 3)$, $(n_C, 3)$ und $(n_A, 7)$ öffentliche RSA Schlüssel von Alice, Bob, Calvin und Dana. Frank verschlüsselt eine Nachricht m mit den öffentlichen Schlüsseln und schickt sie Alice, Bob, Calvin und Dana. Erklären Sie, wie und ob Eve die ursprüngliche Nachricht m in den verschiedenen Fällen bestimmen kann, falls sie die folgenden Informationen erhält:

- (a) Verschlüsselung der Nachricht m gesendet an Alice, Bob und Calvin.
- (b) Verschlüsselung der Nachricht m gesendet an Alice und Dana.
- (c) Verschlüsselung der Nachricht an Alice und Zahlen e und d mit $a^{ed} \equiv a \pmod{n_A}$ für alle $a \in \mathbb{Z}$ mit $\gcd(a, n_A) = 1$.
- (d) Verschlüsselung der Nachricht an Bob und den Wert $\phi(n_B)$.

(6 Punkte)

2. Aufgabe

Argumentieren Sie, warum in dem Polynomring $\mathbb{Z}/n\mathbb{Z}[x]$ mit $n = pq$ und $p, q \in \mathbb{P}$ der euklidische Algorithmus nicht für alle Polynome funktioniert. Geben Sie ein Beispiel dafür an. Erklären Sie, wie man Polynome, bei denen der euklidische Algorithmus nicht anwendbar ist, verwenden kann, um eine Faktorisierung von n zu berechnen.

(4 Punkte)

3. Aufgabe

Sie fangen die beiden Nachrichten $c_1 = 149$ und $c_2 = 253$ ab, die mit RSA durch $c_1 = m_1^3 \pmod{851}$ und $c_2 = m_2^3 \pmod{851}$ verschlüsselt wurden. Von einer zuverlässigen Quelle erfahren Sie, dass $m_2 = 2m_1 + 3$ gilt. Das inspiriert Sie dazu, einen Franklin-Reiter Related Message Angriff durchzuführen, um m_1 zu ermitteln. Falls Sie dabei Kash benutzen wollen, dann könnten die folgenden Befehle nützlich sein:

- $R := \text{ResidueClassRing}(851)$ erzeugt $\mathbb{Z}/851\mathbb{Z}$.

- `PolynomialAlgebra(R)` erzeugt einen Polynomring über dem Ring R .
- In der Polynomalgebra können sie zwar nicht `GCD` aufrufen, aber sie können Polynome `mod` andere Polynome berechnen.

(5 Punkte)

4. Aufgabe

Implementieren RSA, also schreiben Sie ein Programm, dass Schlüsselpaare erzeugt und mit diesen Ver- und Entschlüsselt. Mit `NextPrime()` können Sie sich Primzahlen erzeugen, falls Sie das wollen.

(5 Punkte)