KRY Serie 4

(1) Erstellen Sie für die Klasse `BigInteger` der Package `mybiginteger` eine Spezialversion der Methode `myModPow()` zur Dechiffrierung von RSA-Chiffraten. Dabei sollen der Methode anstelle des RSA-Moduls m dessen beiden Primfaktoren p und q mitgegeben werden, so dass der Algorithmus mit Hilfe des Chinesischen Restsatzes beschleunigt werden kann. Die Deklaration der Methode lautet also wie folgt:

```
public BigInteger myModPow(BigInteger exponent,
                           BigInteger p,
                           BigInteger q).
```

Testen Sie Ihren Algorithmus mit Hilfe des Programms KryptoTrainer „Prakt. 4.1“ in Bezug auf Resultate und zeitliche Effizienz.

(2) ***Hinweis:*** Benutzen Sie für diese Aufgabe die Testumgebung „Prakt. 4.2“ des Programms KryptoTrainer. Die Programmierschnittstelle ist als Kommentar in der Datei `FrameSerie3.java` zu finden.

Gegeben sei eine Datenbank

$$D = [F_1, F_2, F_3, F_4, F_5],$$

mit Datensätzen $F_i \in \mathbb{N}$ von verschiedenen Benutzern B_i (mit $1 \le i \le 5$).

a) (Verschlüsseln der Datenbank D): Erzeugen Sie paarweise verschiedene Primzahlen $p_i > F_i$ (für $1 \le i \le 5$). Berechnen Sie sodann mit Hilfe des Chinesischen Restsatzes die verschlüsselte Datenbank E so, dass $E = F_i \bmod p_i$ (für alle $1 \le i \le 5$).

b) (Entschlüsseln der chiffrierten Datenbank E): Prüfen Sie nach, dass jeder Benutzer B_i mit seinem read-key p_i seinen Datensatz F_i aus dem Chiffrat E rekonstruieren kann (für alle $1 \le i \le 5$).