KRY Serie 6

(1) Erstellen Sie für die Klasse `BigInteger` der Package `mybiginteger` eine `static` Methode

```
public static int[] createTableOfPrimes(int max)
```

welche das `static` Array

```
static int[] tableOfPrimes
```

generiert, das alle Primzahlen enthält, die kleiner oder gleich der Zahl `max` sind.

Der Rückgabewert der Methode soll das Array der Primzahlen sein.

Überprüfen Sie Ihren Algorithmus in der Testumgebung „Prakt. 6“ des Programms KryptoTrainer.

(2) Erstellen Sie für die Klasse `BigInteger` der Package `mybiginteger` eine Methode

```
boolean myIsProbablePrime(int t),
```

welche nach dem Fermat-Test prüft, ob eine gegebene Zahl n zusammengesetzt oder (wahrscheinlich) prim ist.

Der Parameter `t` bezeichne dabei die maximale Anzahl der zufällig gewählten Elemente aus $\mathbf{Z}_n^*$, mit denen der Test durchgeführt werden soll.

Für die Probedivision mit kleinen Primteilern soll die Tabelle aus Aufgabe (1) verwendet werden, falls diese vorhanden ist. Sonst soll keine Probedivision durchgeführt werden. Das Initialisieren der Primzahltabelle soll also der aufrufenden Instanz (in diesem Fall der Testumgebung) überlassen werden (in der Testumgebung ist dazu ein entsprechendes Zahlenfeld vorgesehen).

Überprüfen Sie Ihren Algorithmus in der Testumgebung „Prakt. 6“ des Programms KryptoTrainer.