Mathematik für die Datenkommunikation
Klasse 3Ib

Fachhochschule Nordwestschweiz
Hochschule für Technik

Programmieraufgabe RSA

Ziel der Aufgabe ist es, ein Java-Programm zu erstellen, welches Folgendes leistet:

1. Man kann ein RSA-Schlüsselpaar realistischer Grösse generieren lassen. Dazu ist im Einzelnen zu tun:
   (a) Mit Hilfe der Klasse `BigInteger` sollen zwei unterschiedliche Primzahlen zufällig generiert und multipliziert werden.
   (b) Es soll ein geeignetes e gewählt werden und dazu das passende d bestimmt werden. Dazu ist insbesondere der erweiterte euklidische Algorithmus zu implementieren.
   (c) Der private Schlüssel soll in einer Datei `sk.txt` in der Form (n, d) mit n und d in Dezimaldarstellung abgespeichert werden, der öffentliche in einer Datei `pk.txt` in der Form (n, e).

2. Man kann eine Textdatei (ASCII) `text.txt` in einen String einlesen lassen und diesen String wie folgt verschlüsseln:
   (a) Man liesst einen öffentlichen Schlüssel aus einer Datei `pk.txt` ein.
   (b) Jedes Zeichen von `text.txt` wird in seinen ASCII-Code umgewandelt (Zahl zwischen 0 und 127).
   (c) Jedes Zeichen wird gemäss dem RSA-Verfahren verschlüsselt. Dazu ist insbesondere der Algorithmus der schnellen Exponentiation zu implementieren.
   (d) Die Verschlüsselung erfolgt in eine Datei `chiffre.txt`, wobei die einzelnen Verschlüsselungen in Dezimaldarstellung mit Komma getrennt hintereinander geschrieben werden.

   Bemerkung: Diese zeichenweise Verschlüsselung ist unsicher, da statistische Analysen möglich sind. (Die Buchstabenhäufigkeiten des zu verschlüsselnden Textes übertragen sich auf den Chiffretext.) RSA wird deshalb in der Praxis auch nicht so verwendet. Die genaue Verwendung von RSA wird im Modul "Kryptographie und Informationssicherheit" thematisiert und geht über das in dieser Aufgabe Machbare hinaus.

3. Man kann eine Datei `chiffre.txt`, die wie im obigen Punkt zustande gekommen ist, mit einem privaten Schlüssel aus `sk.txt` entschlüsseln und den resultierenden Text in `text-d.txt` ausgeben.

4. Entschlüsseln Sie die gegebene Datei `chiffre.txt` mit dem gegebenen Schlüssel aus `sk.txt`.

Allgemeine Hinweise:

1. Sie können in Gruppen bis zu drei Personen arbeiten.

2. Bei vollständiger Lösung wird auf die Note des kommenden Tests 0.3 drauf addiert. (Aus systemtechnischen Gründen liegt die Erfahrungsnote zwischen 1.0 und 6.0.)

3. Es ist nicht nötig, das Programm hinsichtlich Effizienz zu optimieren.

4. Das Programm sollte verständlich kommentiert sein.

5. Eigentlich gehe ich davon aus, dass Sie aus Fairnessgründen nicht versuchen, zu betrügen. Dennoch werde ich dies (auch mit Hilfe von Tools) kontrollieren. Falls dabei ein Täuschungsversuch festgestellt wird (also: (verschleierte) Kopien von Teilen existierender Programme (Internet oder Kollegen)), wird die Note des nächsten Tests auf 1.0 gesetzt.

Abgabe: 24.10.23, per Mail. Fügen Sie die Entschlüsselung der von mir gegebenen Datei bei!