Mathematik für die Datenkommunikation
Klasse 3Ib

Fachhochschule Nordwestschweiz
Hochschule für Technik

Programmieraufgabe Elgamal

Erstellen Sie ein Programm in Java welches Folgendes leistet:

1. Sie erstellen aus der folgenden Hexadezimalzahl eine BigInteger Zahl.

   ```
   FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
   29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
   EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
   E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED
   EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D
   C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F
   83655D23 DCA3AD96 1C62F356 208552BB 9ED52907 7096966D
   670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B
   E39E772C 180E8603 9B2783A2 EC07A28F B5C55DF0 6F4C52C9
   DE2BCBF6 95581718 3995497C EA956AE5 15D22618 98FA0510
   15728E5A 8AACAA68 FFFFFFFF FFFFFFFF
   ```

   Mit dieser Zahl n ist $(\mathbb{Z}_n^*, \cdot_n)$ eine zyklische Gruppe und $g = 2$ ist ein Erzeuger dieser Gruppe.

2. Sie schreiben eine Methode, die jeweils den dritten Teil eines öffentlichen und des zugehörigen privaten ElGamal-Schlüssels erzeugt und in Dateien `pk.txt` bzw. `sk.txt` in Dezimaldarstellung speichert. (Die Parameter n und g müssen nicht mit abgespeichert werden, da Sie für die komplette Aufgabe stets die beiden obigen Parameter verwenden sollen. Diese Parameter entsprechen der standardisierten Gruppe MODP-2048).

3. 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 Elgamal-Verfahren verschlüsselt.
   (d) Die Verschlüsselung erfolgt in eine Datei `chiffre.txt`, wobei die einzelnen Verschlüsselungen in der Form (y_1, y_2), wobei y_1 und y_2 jeweils in Dezimaldarstellung sein sollen, mit Strichpunkt getrennt hintereinander geschrieben werden. (Also vom Typ: $(1221, 23323); (232332, 1122); \ldots$)

4. 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.

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

Allgemeine Hinweise:

1. Sie können Gruppen von bis zu drei Personen arbeiten.
2. Für die Exponentiation und das Berechnen des Inversen können Sie entweder die schon in der RSA Aufgabe implementierten Algorithmen oder die entsprechenden BigInteger-Methoden (modPow, modInverse) verwenden.
3. Bei vollständiger Lösung wird auf die Note des kommenden Testes 0.2 drauf addiert.
4. Das Programm sollte verständlich kommentiert sein.
5. **Fügen Sie ihrer Email mit der Abgabe das Resultat der Entschlüsselung von `chiffre.txt` mit dem Schlüssel aus `sk.txt` bei!**
6. **Beachten Sie, dass es sich um Bonuspunkte handelt. Damit können sich interessierte Studierende durch Zusatzarbeit einen kleinen Bonus verdienen. Eigentlich gehe ich davon aus, dass Sie aus Fairnessgründen diesen Studierenden gegenüber 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), wird die Note des nächsten Tests auf 1.0 gesetzt.**

Abgabe: 10.12.2023