KRY: Wahlfach Kryptologie
Serie 7: Public Key Systeme, Faktorisierungen

Aufgabe 1 (T)
Wir betrachten die Primzahl $p = 107$. Bob und Alice führen den Diffie-Hellman-Schlüsselaustausch mit p und der Primitivwurzel $g = 2 \pmod p$ durch. Die Zufallszahl von Alice ist $a = 66$, diejenige von Bob ist $b = 33$. Bestimmen Sie den gemeinsamen Schlüssel.

Aufgabe 2 (T)
Alice wählt für das El Gamal Verfahren den öffentlichen Schlüssel ($p = 31$, $g = 3$, $A = 17$), ihr geheimer Schlüssel ist $a = 7$. Bob will mit Hilfe dieses Schlüssels $m = 9$ an Alice schicken und wählt $b = 12$.

Bestimmen Sie den Schlüsseltext und entschlüsseln Sie den Text anschliessend.

Aufgabe 3 (T)
Wir setzen $n = 59'153$. Faktorisieren Sie n mit Hilfe von Pollard's ρ-Algorithmus. Starten Sie dazu mit $x_0 = 24'712$, und setzen Sie $a = 1$.

Aufgabe 4 (P)
Programmieren Sie für die Klasse BigInteger die folgenden Methoden. Überprüfen Sie Ihren Algorithmus in der Testumgebung "Prakt. 7" des Programms KryptoTrainer.

(1) Die Hilfs-Methode `findExp`, die für gegebene natürliche Zahlen z und r das maximale ganzzahlige x bestimmt, so dass $z^x \leq r$.
Hinweis: Da die Werte von z und r in den Aufrufen jeweils relativ klein sind, können Sie diese in den Typ `double` konvertieren und dann den Befehl `Math.log()` auf geeignete Art einsetzen.

Testen Sie die Methode mithilfe einiger selbst gewählten Eingaben im GUI.

(2) Die Methode `findFactor`, die mithilfe der $(p-1)$-Methode einen Faktor von einer gegebenen natürlichen Zahl n sucht. Gegeben ist ausserdem eine natürliche Zahl B, die gemäss der Beschreibung im Skript die Obergrenze für die einzelnen Faktoren bildet.
Hinweis: Testen Sie das Programm mit der Eingabe: $n = 695256$, $B = 100$. Die Ausgabe sollte einen Faktor von n ergeben.

Aufgabe 1:
A = g^a mod p = 2 ^ 66 mod 107 = 47
B = g^b mod p = 2 ^ 33 mod 107 = 58

K = B^a mod p = 58 ^ 66 mod 107 = 75
K = A^b mod p = 47 ^ 33 mod 107 = 75 -> Gemeinsamer Schlüssel ist 75!

Aufgabe 2:

Alice w¨ahlt fur¨ das El Gamal Verfahren den ¨offentlichen Schlussel¨ (p = 31, g = 3, A = 17), ihr geheimer Schlussel¨ ist a = 7. Bob will mit Hilfe dieses Schlussels¨ m = 9 an Alice schicken und w¨ahlt b = 12.
Bestimmen Sie den Schlusseltext¨ und entschlusseln¨ Sie den Text anschliessend.

A = g^a mod p = 3 ^ 7 mod 31 = 17
B = g^b mod p = 3 ^ 12 mod 31 = 8

c = A^b * m mod p = 17 ^12 * 9 mod 31 = 18

Schlüsseltext = (8,18)

Entschlüsselung: c * B^(p-1-a) = 18 * 8 ^ (31-1-7) = 18 * 8 ^ 23 mod 31 = 9

Aufgabe 3:

Wir setzen n = 59'153. Faktorisieren Sie n mit Hilfe von Pollard's ρ-Algorithmus. Starten Sie dazu mit x0 = 24'712, und setzen Sie a = 1.

xi := (xi−1)^2+1 (mod n) und yi := ((yi−1)^2+1)^2+1 (mod n)

x0 = 24'712, y0 = 24'712, ggt(y0-y0,n) = ggt(0, 59'153) = 1

x1 = (24'712^2 + 1) mod 59'153 = 46'526, y1 = ((24'712^2 + 1) ^ 2 + 1) mod 59'153 = 23'795, ggt(22731,n) = 1

x2 = (46'526^2 + 1) mod 59'153 = 23'795, y1 = ((23'795^2 + 1) ^ 2 + 1) mod 59'153 = 15'521, ggt(8274,n) = 1

x3 = (23'795^2 + 1) mod 59'153 = 48'663, y1 = ((15'521^2 + 1) ^ 2 + 1) mod 59'153 = 56'180, ggt(x-y,n) = 1

x4 = (48'663^2 + 1) mod 59'153 = 15'521, y1 = ((56'180^2 + 1) ^ 2 + 1) mod 59'153 = 15'613, ggt(x-y,n) = 1

x5 = (15'521^2 + 1) mod 59'153 = 30'426, y1 = ((15'613^2 + 1) ^ 2 + 1) mod 59'153 = 49'942, ggt(x-y,n) = 1

x6 = (30'426^2 + 1) mod 59'153 = 56'180, y1 = ((49'942^2 + 1) ^ 2 + 1) mod 59'153 = 50'439, ggt(5741,n) = 1

x7 = (56'180^2 + 1) mod 59'153 = 24'933, y1 = ((50'439^2 + 1) ^ 2 + 1) mod 59'153 = 11'927, ggt(13'006,n) = 1

x8 = (24'933^2 + 1) mod 59'153 = 15'613, y1 = ((11'927^2 + 1) ^ 2 + 1) mod 59'153 = 22'169, ggt(x-y,n) = 149

Faktor = 149