# 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 $\rho$-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.

1) $p = 107$ ; $a = 66$ ; $b = 33$ ;

$g = 2 \pmod{p}$

$A = g^a \qquad B = g^b$

$B^a = g^{ab} \qquad A^b = g^{ab}$

$\rightarrow 2^{33 \cdot 66} \bmod 107$

$= \underline{75}$

```
(07:57) gp > Mod(2^(33*66),107)
%2 = Mod(75, 107)
```

$p = 31$ ; $g = 3$ ; $A = 17$ ; $a = 7$ ; $b = 12$ ;

2) $m = 9 \quad A = g^a \quad B = g^b = 3^{12} \bmod 31 = 8$

$c = A^b \cdot m = 17^{12} \cdot 9 \bmod 31 = 18$ ← Verschlüsselung

$m = c \cdot B^{p-1-a} = c \cdot (g^b)^{31-1-7} \bmod 31 = 9$ ← Entschlüsselung

3) $n = 59'153 \qquad x_0 = 24'712 = y_0$

$a = 1$

1. Wähle $x_0 = y_0$ und $a$ ($\neq 0, -2$) zufällig, setze $i := 1$.
2. **while** (noch keine Kollision gefunden)
   - 2.1 Bestimme $x_i := (x_{i-1})^2 + a \pmod{n}$,
     und $y_i := ((y_{i-1})^2 + a)^2 + a \pmod{n}$
   - 2.2 $d := \mathrm{ggT}(x_i - y_i, n)$
   - 2.3 **if** $(1 < d < n)$ **return** $d$
   - 2.4 $i := i + 1$

**end**

- Gemäss Def: $x_i := f(x_{i-1}) = x_{i-1}^2 + a \pmod{n}$
- Einsetzen ergibt:
  $y_i = x_{2i} = x_{2i-1}^2 + a = (x_{2i-2}^2 + a)^2 + a = (y_{i-1}^2 + a)^2 + a \pmod{n}$

x1 = x0^2+a mod n = 46526
y1 = (y0^2+a)^2+a mod n = 23795
gcd(x0-y0,n) = 1

x2 = x1^2+a mod n = 23795
y2 = (y1^2+a)^2+a mod n = 15521
gcd(x2-y2,n) = 1

x3 = x2^2+a mod n = 48663
y3 = (y2^2+a)^2+a mod n = 56180
gcd(x3-y3,n) = 1

x4 = x3^2+a mod n = 15521
y4 = (y3^2+a)^2+a mod n = 15613
gcd(x4-y4,n) = 1

x5 = x4^2+a mod n = 30426
y5 = (y4^2+a)^2+a mod n = 49942
gcd(x5-y5,n) = 1

x6 = x5^2+a mod n = 56180
y6 = (y5^2+a)^2+a mod n = 50439
gcd(x6-y6,n) = 1

x7 = x6^2+a mod n = 24933
y7 = (y6^2+a)^2+a mod n = 11927
gcd(x7-y7,n) = 1

x8 = x7^2+a mod n = 15613
y8 = (y7^2+a)^2+a mod n = 22169
gcd(x8-y8,n) = 149