



Angewandte Kryptographie – Übung 4

Aufgabe 1 (ElGamal Grundlagen)

Implementieren Sie das ElGamal-Kryptosystem. Hierzu definiere man eine Klasse ElGamal, die als Attribute die `BigInteger`-Werte p, g, a und die im folgenden beschriebenen Methoden enthält.

- setup* erzeuge für vorgegebene Bitlänge die 3 Parameter.
- encrypt* verschlüssele ein Element aus $\mathbf{Z}/p\mathbf{Z}$.
- decrypt* entschlüssele ein Element aus $\mathbf{Z}/p\mathbf{Z}$.

Für eine vorgegebene Bitlänge b sollten Sie p folgendermaßen wählen:

- wähle eine Primzahl q der Bitlänge $b - 1$
- prüfe, ob $p = 2q + 1$ eine Primzahl ist, falls ja \leadsto fertig
- falls p keine Primzahl ist, so wähle ein neues q

Dann ergibt sich nämlich die Primfaktorzerlegung von $p - 1$ sehr einfach als $p - 1 = 2 \cdot q$ und das Erzeugerkriterium für g ist ein kurzer Test mit Hilfe von zwei Potenzierungen.

Lesen Sie die Bitlänge von der Kommandozeile ein und testen Sie mit Hilfe der *decrypt*-Methode, ob die *encrypt* Methode korrekt arbeitet.