## 4.5 ElGamal-Chiffrierung – Idee

Die ElGamal-Chiffre ist ein asymmetrisches Verfahren – genauer gesagt ein hybrides –, das ebenfalls auf der Komplexität des diskreten Logarithmus beruht.

Eine Primzahl $p$ und ein $g \in [2 \dots p-2]$ sind öffentlich festgelegt; $g$ sollte von hoher Ordnung, am besten primitives Element sein.

> $p$ und $g$ können für alle Teilnehmer gemeinsam gelten, können aber auch individuell verschieden sein.

Jeder Teilnehmer wählt sich eine zufällige Zahl

$$d \in [2 \dots p-2]$$

als privaten Schlüssel und bildet daraus

$$e = g^d \bmod p$$

als zugehörigen öffentlichen Schlüssel. Die Bestimmung von $d$ aus $e$ bedeutet gerade die Berechnung eines diskreten Logarithmus.

Wie soll man nun eine Nachricht $a$ so transformieren, dass sie nur mit Kenntnis von $d$ wiederzugewinnen ist? Die naive Idee, $e^a = g^{da} \bmod p$ zu schicken, nützt nichts – auch der Empfänger kann trotz Kenntnis von $d$ die Nachricht $a$ nicht entschlüsseln. Auch $r = g^a \bmod p$ zu schicken, nützt nichts – der Empfänger kann nur $r^d = e^a \bmod p$ bestimmen, aber nicht $a$.

Eine bessere Idee ist, erst einen Schlüssel zu erzeugen, mit dem dann ein hybrides Verfahren durchgeführt wird:

- Alice wählt ein zufälliges $k \in [2 \dots p-2]$. Als Schlüssel soll $K = e^k \bmod p$ mit dem öffentlichen Schlüssel von Bob verwendet werden; dieses kann Alice berechnen.
- Damit auch Bob den Schlüssel $K$ bestimmen kann, schickt Alice mit ihrer Nachricht die *Schlüssel-Information* $r = g^k \bmod p$ mit.
- Bob kann daraus $r^d = g^{kd} = e^k = K \bmod p$ mit Hilfe seines privaten Schlüssels $d$ berechnen.

Als symmetrische Chiffe beim Hybridverfahren wird die Verschiebechiffre auf $\mathbb{F}_p^\times$ genommen, wobei $K$ als Einmalschlüssel dient – d. h., für jeden Klartextblock ist ein neuer Schlüssel $K$ zu erzeugen und die entsprechende Schlüssel-Information mitzuschicken. Dadurch ist die Länge des Geheimtexts gerade das Doppelte der Länge des Klartexts.

Die Verschlüsselung läuft dann nach Bildung des Schlüssels und der Schlüssel-Information so weiter ab:

- Alice berechnet den Geheimtext $c = Ka \bmod p$ und schickt diesen zusammen mit $r$ an Bob.

Die Entschlüsselung ist dann, nachdem Bob den Schlüssel $K$ wie oben beschrieben berechnet hat:

- $a = K^{-1}c \bmod p$ durch Kongruenzdivision.