Das Problem: Alice (A) möchte Bob (B) eine Nachricht $\mathfrak{m}$ senden, ohne dass andere diese lesen können.

$$\text{Alice} \xrightarrow{\text{Nachricht } \mathfrak{m}} \text{Bob}$$

Idee: A verschlüsselt die Nachricht so, dass nur B sie (in vernünftiger Zeit) entschlüsseln kann.

In *asymmetrischen Kryptosystemen* werden eingesetzt:

- **elliptische Kurven** = abelsche Varietäten der Dimension 1
- **Jakobische hyperelliptischer Kurven:** Dies sind spezielle abelsche Varietäten mit einer Prinzipal-Polarisierung, d.h. einer Polarisierung vom Typ $(1, \ldots, 1)$
  [Kobliz, 1989]
- **Prymvarietäten:** spezielle abelsche Varietäten, die als Untervarietäten von Jakobischen auftreten
  [Seßler, 2006]

Man arbeitet dabei über *endlichen* Körpern K.

Die ElGamal-Verschlüsselung (ElGamal, 1985)

(1) B wählt
- eine hyperelliptische Kurve C über einem endlichen Körper K,
- einen Divisor D vom Grad 0 auf C,
- eine Zahl $b \in \mathbb{Z}$.

Wir betrachten D in

$$\mathrm{Jac}(C) \cong \mathrm{Pic}^0(C) := \mathrm{Div}^0(C) \Big/ \equiv_{\mathrm{lin}}$$

Es ist $X := \mathrm{Jac}(C)$ eine abelsche Varietät.

(2) B berechnet bD (durch b-fache Addition in X).

(3) B gibt die Daten (C, K, D, bD) als *öffentlichen Schlüssel* bekannt. Er hält aber b geheim.

(4) A holt sich (C, K, D, bD).
A wählt zufällig $a \in \mathbb{Z}$.
A berechnet aD und $a(bD)$.

(5) A wandelt die (textuelle) Nachricht m in eine Divisorklasse $M \in \mathrm{Jac}(C)$ um
(z.B. nach der Methode von Göb 2004).
A berechnet $M' := M + a(bD)$ (**Verschlüsselung**)
und sendet M' und aD an B.

(6) B berechnet $M' - b(aD) = M + a(bD) - b(aD) = M$
(**Entschlüsselung**)

Bemerkungen:

- Jemand, der $\mathfrak{b}$ kennt, könnte nach Abhören von $\mathfrak{M}'$ und $\mathfrak{a}\mathfrak{D}$ die Nachricht ebenfalls entschlüsseln.
- Er müsste $\mathfrak{b}$ aus $\mathfrak{D}$ und $\mathfrak{b}\mathfrak{D}$ berechnen.
- Das Verfahren beruht darauf, dass
  - Addition und Vervielfachen von Divisoren leicht (in polynomialer Zeit) möglich ist, während
  - für die Berechnung von $\mathfrak{b}$ aus $\mathfrak{D}$ und $\mathfrak{b}\mathfrak{D}$ nur exponentielle Algorithmen bekannt sind (DLP bzw. HCDLP, siehe unten)

Das Problem des diskreten Logarithmus (DLP).
Sei G eine endliche abelsche Gruppe der Ordnung $\mathfrak{n}$.
Sind $\mathfrak{g}, \mathfrak{g}' \in G$ mit $\mathrm{ord}(\mathfrak{g}) = \mathfrak{n}$, so heißt eine ganze Zahl $\mathfrak{m}$ mit $0 < \mathfrak{m} < \mathfrak{n}$ und

$$\mathfrak{g}' = \mathfrak{m}\mathfrak{g}$$

ein *diskreter Logarithmus* von $\mathfrak{g}'$ zur Basis $\mathfrak{g}$.

Beispiel 1: Multiplikative Gruppe $G := (\mathbb{Z}/\mathfrak{p}\mathbb{Z})^*$
Zu $\mathfrak{g}, \mathfrak{g}' \in G$ ist ein $\mathfrak{m} < \mathfrak{p}$ zu finden mit $\mathfrak{g}^{\mathfrak{m}} = \mathfrak{g}'$.

Beispiel 2: DLP für hyperelliptische Kurven (HCDLP).
Sei C eine hyperelliptische Kurve über einem endlichen Körper.
$G := \mathrm{Jac}(C)$