- Das RSA-Verfahren ist sehr sicher, denn man kann die Vorschrift, wie man die Nachricht wieder entschlüsseln kann, nicht oder nur mit einem riesigem Zeitaufwand (in der Größenordnung von Jahren, selbst wenn man moderne Hochleistungsrechner zu Hilfe nimmt) herausbekommen.

Diese letzte Bedingung lässt sich mit dem Begriff der *Einwegfunktion* beschreiben:

Definition 3.1 *Eine Einwegfunktion ist eine Abbildung f einer Menge X in eine Menge Y, so dass $f(x)$ für jedes Element von X leicht zu berechnen ist, während es für (fast) jedes y aus Y extrem schwer ist, ein Urbild x (d.h. ein x mit $f(x) = y$) zu finden.*

Beispiele für Einwegfunktionen sind das Telefonbuch und der Briefkasten:

- Das Telefonbuch ordnet jedem Namen eine Telefonnummer zu. Um aus der Telefonnummer aber auf den Namen zurückschließen zu können, müsste man die Einträge einzeln durchlesen (solange man sich nicht eines elektronischen Telefonbuchs mit Suchfunktion bedient).
- Man kann leicht eine Nachricht in einen Briefkasten einwerfen. Den Briefkasten öffnen und damit die Nachricht lesen kann jedoch nur, wer den privaten Schlüssel für seinen Briefkasten besitzt.

Zum Verständnis des Begriffs dient das Arbeitsblatt *Einwegfunktionen*.

Arbeitsblatt: Einwegfunktionen

Als *Einwegfunktion* bezeichnet man eine Abbildung f von einer Menge X in eine Menge Y, für die $f(x)$ für jedes Element von x leicht zu berechnen ist, während es für (fast) jedes $y \in Y$ extrem schwer ist, ein Urbild x (d.h. ein $x \in X$ mit $f(x) = y$) zu finden.

Aufgaben:

1. Inwiefern entspricht das Telefonbuch einer Einwegfunktion?

2. Beschreibe, inwiefern die folgenden Vorgänge Einwegfunktionen entsprechen:
   (a) Erbsen und Linsen mischen
   (b) Farben mischen
   (c) Geld ausgeben
   (d) Sand und Kies mischen

3. Eine spezielle Variante von Einwegfunktionen sind die *Trapdoor-Einwegfunktionen* (trapdoor = Geheimtür), die sich nur dann einfach lösen lassen, wenn man eine (geheime) Zusatzinformation besitzt. Erkläre, inwiefern ein Briefkasten als Bild für eine Trapdoor-Einwegfunktion angesehen werden kann.

Mathematische Beispiele für Einwegfunktionen:

- Die Multiplikation zweier (großer) Primzahlen ist einfach, während die Umkehrung (d.h. die Primfaktorzerlegung) schwer (aufwändig) ist.

- Quadrieren modulo n, wobei n das Produkt zweier großer Primzahlen p und q ist.