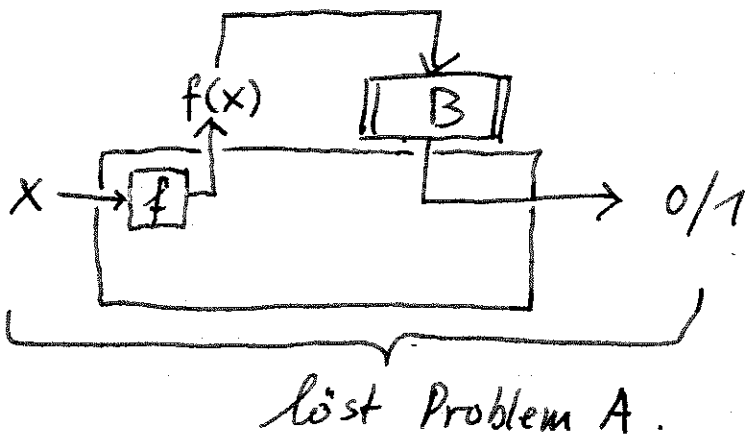
Aufgabe: Normalerweise definiert man polynomiale Reduzierbarkeit von A nach B so: es muss eine polynomial-berechenbare Funktion f geben, so dass gilt:

$$\forall x : (x \in A \iff f(x) \in B)$$

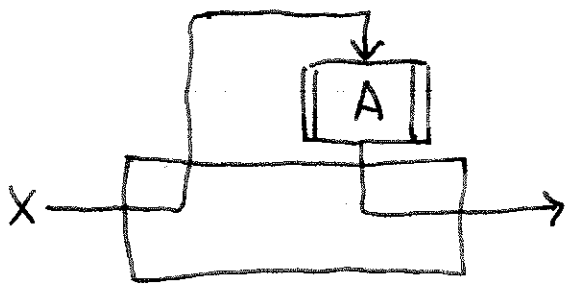
Man zeige, dass diese Art der Reduzierbarkeit von A nach B impliziert, dass $A \leq_{eff} B$.

Beweis durch Skizze:



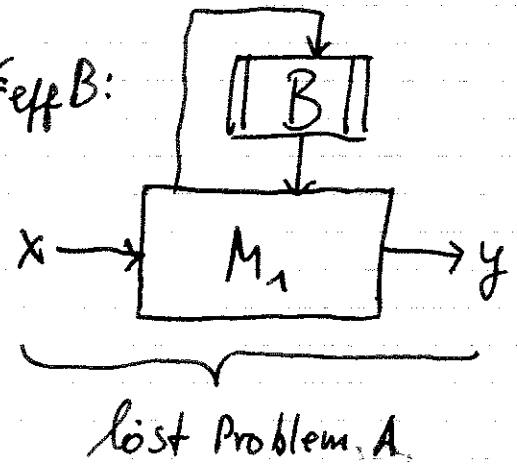
Aufgabe: Man zeige, dass die Relation $\leq_{eff}$ reflexiv und transitiv ist.

Beweis durch Skizze (Reflexivität):

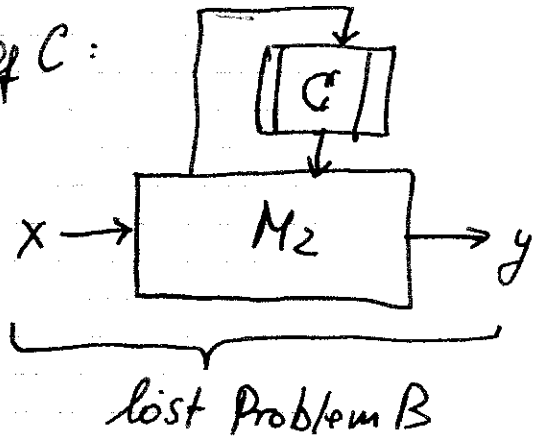


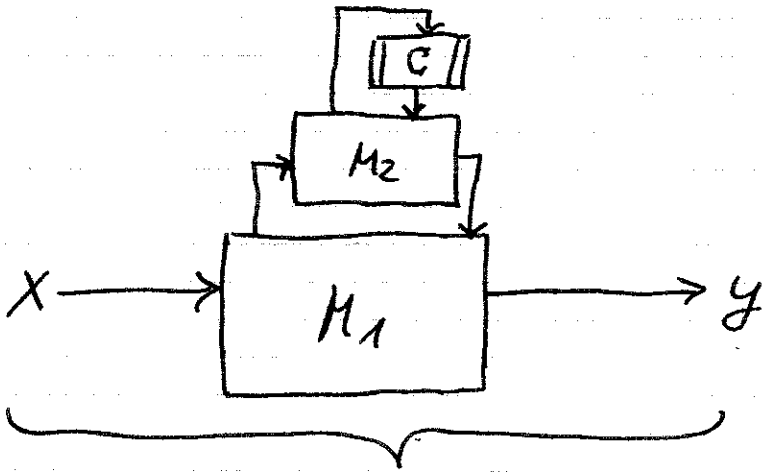
Beweis der Transitivität durch Skizze:

$A \leq_{\text{eff}} B$:



$B \leq_{\text{eff}} C$:





also: $A \leq_{\text{eff}} C$.

Der Basisalgorithmus hier, der aus M_1 und M_2 besteht, ist immer noch polynomial.

Eine Einwegfunktion (one-way function) ist eine Funktion f, die in Vorwärtsrichtung $x \overset{f}{\longmapsto} y$ effizient berechenbar ist, jedoch nicht in Rückwärtsrichtung. Dies ist die informale Idee.

Typische kryptographische Verwendung von Einwegfunktion:

Man wählt x zufällig, berechnet $y = f(x)$.

x bleibt geheim, y wird veröffentlicht.

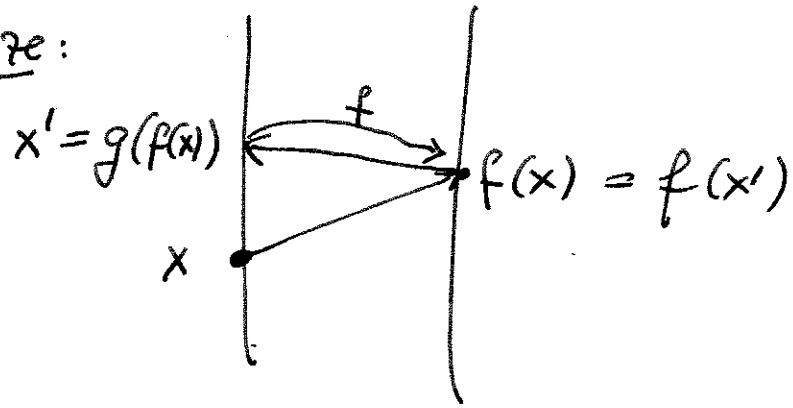
Oder: Computersystem hat verschiedene Benutzer, die sich mit einem Passwort einloggen. Es ist gefährlich, die Benutzernamen samt Passwörter zu speichern. Stattdessen speichert man für jeden Benutzer b mit Passwort x_b den Wert $f(x_b)$. Diese Liste $(b, f(x_b)), \ldots$ kann sogar öffentlich zugänglich sein. Meldet sich Benutzer b mit Passwort x an, so überprüft das System, ob $(b, f(x))$ in der Liste gespeichert ist.

Formale Definition (erster Versuch):

f heißt Einwegfunktion, falls $f \in \mathbb{P}$ (d.h. das Berechnen von $x \xrightarrow{f} y$ geht in der Zeit $p(|x|)$, wobei p ein Polynom ist).

Es gibt keine effizient berechenbare Funktion g mit der Eigenschaft $f(g(f(x))) = f(x) \quad \forall x$.

Skizze:



D.h. g liefert, angesetzt auf $f(x)$, irgendein Urbild von $f(x)$, nicht notwendigerweise x.

Weitere Bedingung an f: es gibt ein Polynom q so dass für alle x gilt: $q(|f(x)|) \geq |x|$.

Satz: Es existieren Einwegfunktionen gdw.

$$P \neq NP.$$

Beweis: Angenommen, $P = NP$. Dann gibt es für alle NP-Probleme einen polynomialen Algorithmus. Speziell auch für die folgende Sprache, die in NP liegt:

$$A_f = \{(u, y) \mid \text{es gibt } v \text{ so dass } f(uv) = y\}$$

Hierbei sei f eine beliebige, effizient berechenbare Fkt.
Wegen $P = NP$ liegt A in P. Der folgende polynomiale Algorithmus berechnet eine Umkehrfunktion g von f:

Eingabe y $(= f(x))$

$u := \varepsilon$

repeat

if $(u1, y) \in A_f$ then $u := u1$

if $(u0, y) \in A_f$ then $u := u0$

until $f(u) = y$

output u

Daher kann es keine Einwegfunktion geben.
Umgekehrt, sei angenommen $P \neq NP$. Dann ist das NP-vollständige Problem SAT nicht in P.
Definiere folgende Funktion f:

$$f(G, y) = \begin{cases} (G, 1), & \text{wenn } y \text{ die Boole'sche Formel } G \text{ erfüllt,} \\ (G, 0), & \text{sonst} \end{cases}$$

f ist effizient berechenbar. Wenn man bzw. g wie in Def. beschrieben
f^{-1} effizient berechnen könnte, also insbesondere für erfüllbare Formeln G gilt:

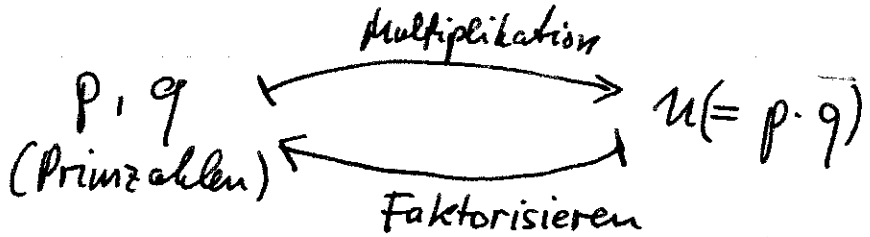
$(G, 1) \longmapsto (G, y)$ wobei y erfüllende Belegung für G ist

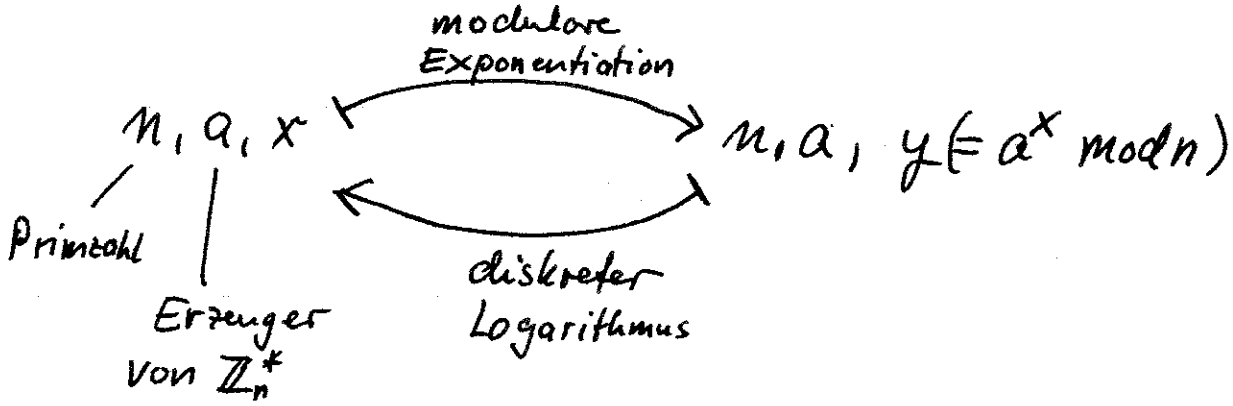
dann wäre $SAT \in P$, Widerspruch.
Also kann keine Umkehrfunktion g wie in Def. beschrieben effizient berechenbar sein. Daher existiert eine Einwegfunktion, nämlich f wie oben definiert. □

Tatsächlich sind in Kryptographie noch härtere Bedingungen an die Einwegfunktion f zu stellen.

Def (starke Einwegfunktion)
- f ist effizient berechenbar ($f \in P$)
- f ist injektiv
- Es gibt Polynom p so dass $\forall x \; p(|f(x)|) \geq |x|$
- Für jede polynomial berechenbare Fkt. g und für jedes Polynom p hat die Menge $S = \{x \mid g(f(x)) = x\}$ folgende „Dichte": $\frac{|S|}{2^n} \leq \frac{1}{p(n)}$ (wobei $S \subseteq \{0,1\}^n$)

Kandidaten für Einwegfunktionen:



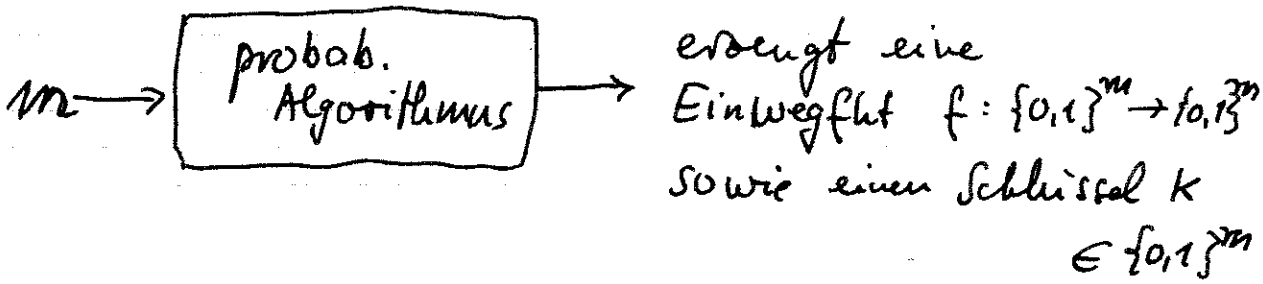


Vermutlich sogar starke Einwegfunktionen.

Fazit: Die Existenz von Einwegfunktionen, wie sie in der Kryptographie benötigt werden setzt noch stärkere Annahmen als $P \neq NP$ voraus (und nicht einmal $P \neq NP$ ist bis jetzt bewiesen).

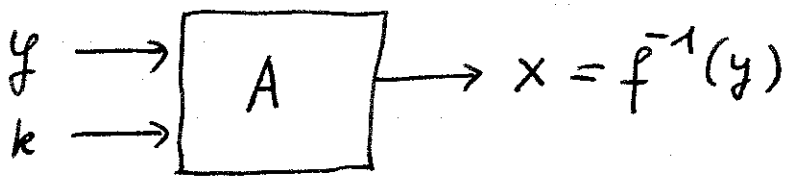
Manche kryptographische Anwendungen benötigen eine Einwegfunktion mit Falltür (one way trapdoor function).

Nehmen wir an $|x| = |f(x)| =: n$. Ferner gibt es einen Schlüssel, ebenfalls der Länge n.



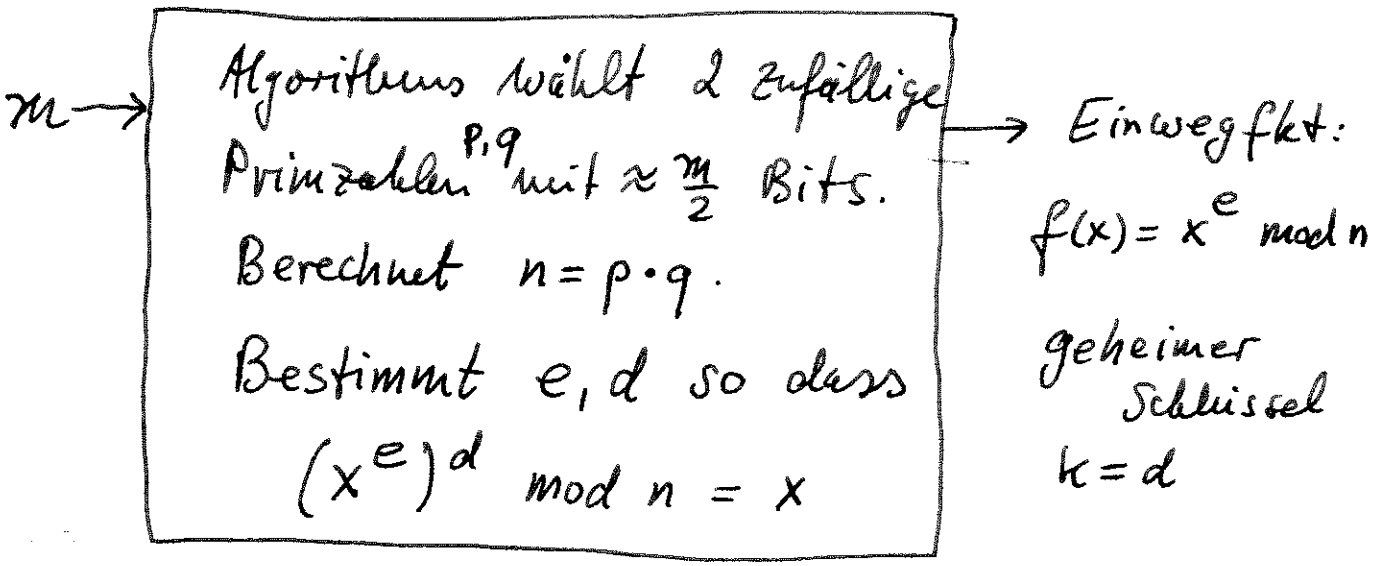
Mit Hilfe des Schlüssels k sollte es möglich sein, f zu invertieren. D.h. es gibt effizienten Algorithmus A so dass

$\forall y = f(x)$:



Ohne Kenntnis von k kann x aus y nicht berechnet werden.

Vorschau (später ausführlicher): RSA verwendet eine Einwegfunktion mit Falltür:



Alle hier beteiligten Zahlen $n, e, d, x, f(x)$ bestehen aus $\approx m$ Bits.

Manche Anwendungen benötigen <u>homomorphe</u> Einwegfunktion $f: A \to B$. (→ Zero Knowledge)

Das bedeutet: Sowohl auf A als auch auf B besteht eine Gruppenstruktur: $(A, \circ)$ und $(B, \bullet)$

Dann sollte gelten: $f(x \circ y) = f(x) \bullet f(y)$

<u>Bsp 1</u>: Die Exponentialfunktion $x \mapsto f(x) = a^x$ (ggf. modulo einer Primzahl n)

Dann gilt: $f(x+y) = a^{x+y} = a^x \cdot a^y = f(x) \cdot f(y)$

<u>Bsp 2</u>: Die Quadratfunktion $x \mapsto sqr(x) = x^2$ (evtl. mod n)

$$sqr(x \cdot y) = (x \cdot y)^2 = x^2 \cdot y^2 = sqr(x) \cdot sqr(y)$$

Restklassen

Äquivalenzrelation auf $\mathbb{Z}$: $\equiv_k$ $(k \in \mathbb{N})$

bedeutet: $x \equiv_k y$ (andere Schreibweise: $x \equiv y \pmod{k}$)

$x - y$ ist durch k teilbar.

$\mathbb{Z}$ wird in Äq.klassen zerlegt, z.B. $\equiv_5$

$[5] = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$

$[-9] = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$

$[2] = \{\ldots, -3, 2, 7, 12, \ldots\}$

$[13] = \{\ldots, -2, 3, 8, 13, \ldots\}$

$[-1] = \{\ldots, -1, 4, 9, 14, \ldots\}$

$5, -9, 2, 13, -1$ ist vollständiges Repräsentantensyst. (Restsystem)

$0, 1, 2, 3, 4$ ist ——"—— kanonisches ——"——

(evtl: $-2, -1, 0, 1, 2$)

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$$

Kurz: $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$(\mathbb{Z}_n, +_{\bmod n})$ ist kommut. Gruppe.

$(\mathbb{Z}_n, *_{\mod n})$ ist i.A. keine Gruppe

$x \in \mathbb{Z}_n$ hat multipl. Inverses $(\exists y: x \cdot y \equiv 1 \pmod n)$

gdw.

$ggT(x,n) = 1$

$\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \mid ggT(x,n) = 1\}$ $\quad (\mathbb{Z}/n\mathbb{Z})$

z.B: $\mathbb{Z}_{12}^* = \{\underbrace{1, 5, 7, 11}\}$

reduziertes Restsystem

$\varphi(n) = |\mathbb{Z}_n^*|$ Eulersche Phi-Funktion

n Primzahl $\Leftrightarrow$ $\mathbb{Z}_n^* = \{1, 2, \ldots, n-1\}$

$\Leftrightarrow$ $\varphi(n) = n-1$

$(\mathbb{Z}_n, +, *)$ ... Körper $\begin{cases} (\mathbb{Z}_n, +) \text{ komm. Gruppe} \\ (\underbrace{\mathbb{Z}_n \setminus \{0\}}_{\mathbb{Z}_n^*}, *) \text{ Gruppe} \\ \text{Distributivgesetz: } x*(y+z) = x*y + x*z \pmod n \end{cases}$

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$2^1 = \underline{2}, \; 2^2 = \underline{4}, \; 2^3 = 8 = \underline{3}, \; 2^4 = 6 = \underline{1}$