Das RSA Verfahren

Um die Funktionsweise des RSA Verfahrens nachzuvollziehen, musst du dir Klartext, Geheimtext und Schlüssel nicht als Bit-Folgen wie bei AES, sondern einfach als natürliche Zahlen vorstellen. Für den Computer macht das sowieso keinen Unterschied, da dieser alle Daten als Bit-Folge abspeichert udn verarbeitet.

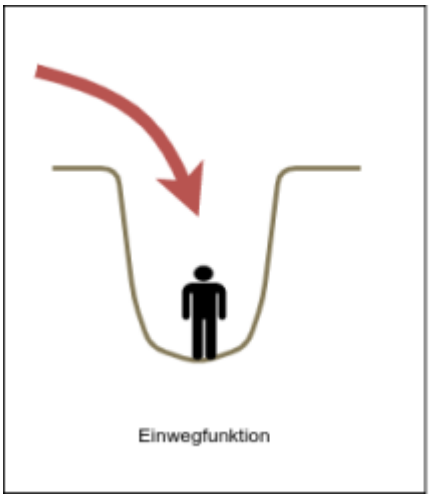
Einwegfunktionen und Falltürfunktionen

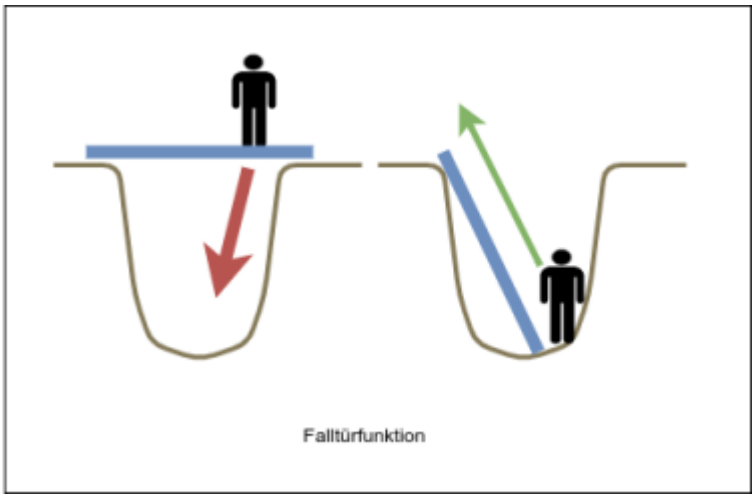
Im vorigen Wiki-Abschnitt haben wir uns mit der Modulo-Rechnung beschäftigt - diese ist in der Kryptografie wichtig, da einge der Modulo-Rechenarten sind sehr **einfach durchgeführt** werden können, ihre **Umkehrung** oft aber sehr ziemlich **aufwändig** ist.

So kann man die **einfache Rechnung als Verschlüsselung** und die **komplizierte Umkehrung als Entschlüsselung** verwenden – allerding nur dann, wenn es bei der komplizierten Umkehrung eine "versteckte Abkürzung" gibt, die man als **Schlüssel** nehmen kann.

Eine Funktion, die man einfach berechnen kann, bei der die Umkehrung aber nur mit großem Aufwand berechnet werden kann, nennt man **Einwegfunktion**.

Existiert eine "versteckte Abkürzung", also eine Zusatzinformation, mit der die ansonsten schwierige Umkehrung einfach gemacht wird, dann spricht man von einer **Falltürfunktion**.





Primzahl-Multiplikation als Einwegfunktion

Die (normale) Multiplikation zweier Primzahlen ist eine Einwegfunktion. Eine Primzahl-Multiplikation ist heutzutage mit Computerunterstützung einfach durchführbar, auch bei großen Zahlen macht das keine Probleme.

Im Gegensatz dazu sind keine effizienten Verfahren bekannt, mit denen aus dem Produkt zweier großer Primzahlen die beiden Faktoren bestimmt werden können.

(A1)

- Berechne im Kopf 13·17
- Bestimme die beiden Primzahlen, die miteinander multipliziert 1189 ergeben (auch im Kopf...)

Je größer die beiden Primzahlen sind, desto komplexer ist dieses sogenannte **Faktorisierungsproblem**: "Finde die beiden Primzahlen, die miteinander multipliziert die Zahl X ergeben". Bei Zahlen über tausend Bit Länge ist dieses Problem auch von aktuellen Superrechnern nicht mehr lösbar.

Die **Multiplikation zweier großer Primzahlen ist eine Einwegfunktion**. Es ist **einfach, das Produkt zu berechnen**, aber sehr **schwierig/unlösbar**, zu einer großen Zahl **die beiden Prim-Faktoren zu bestimmen**, die miteinander multipliziert diese Zahl ergeben.

Anmerkungen:

- Es lässt sich mathematisch nicht beweisen, dass dass die Primzahl-Multiplikation eine Einwegfunktion ist, es spricht jedoch alles dafür.
- Ein zentrales Problem dieser Einwegfunktion ist die Erzeugung großer Primzahlen. Das wird meist mit dem Miller-Rabin-Test gelöst, dessen Betrachtung hier aber zu weit führen würde.

Aus Einweg mach Falltür

Des RSA Verfahren basiert darauf, eine passende Falltürfunktion zu finden, die bei geeignet Wahl der beteiligten Zahlen eine Information als Schlüssel liefert, mit der sie umgekehrt werden kann.

Dazu benötigt man die Modulo-Rechnung aus einem der vorigen Wiki-Abschnitte:

- Die a-te Wurzel der Zahl b modulo n lässt sich leicht berechnen, wenn man φ(n) kennt und a und $φ(n)$ teilerfremd sind. (Modulo-Wurzelziehen)
- φ(n) kann man leicht berechnen, wenn es sich bei n um das Produkt zweier Primzahlen p und q handelt. Dann gilt φ(n)=(p-1)·(q-1) (Modulo-Wurzelziehen)

Nach heutigem Kenntnisstand gibt es außer der im Abschnitt Modulo-Wurzelziehen beschriebenen Methode unter Zuhilfenahme von $φ(n)$ keine effektive Methode, die Modulo-Wuzel zu bestimmen. Damit ist das Modulo-Potenzieren eine Falltürfunktion - die Information, die sie umkehrbar macht sind die beiden Primzahlfaktoren aus denen der Modulus n berechnet werden kann. Da die

Primzahlmultiplikation eine Einwegfunktion ist, kann man diese Faktoren nachträglich aus n bei genügend großen Primzahlen nicht mehr bestimmen.

$$m^e = c \ (mod\ n)$$

Wenn $\varphi(n)$ nicht bekannt und teilerfremd zu a ist, kann man m nicht aus Kenntnis von e, c und n bestimmen.

Mit n und e kann die Nachricht **m** in den Geheimtext **c** überführt werden (aber nicht mehr aus c m bestimmt werden!)

Wähle $n = p \cdot q$ mit großen Primzahlen p und q sowie eine Zahl e die teilerfremd zu $\varphi(n) = (p-1) \cdot (q-1)$ ist.

(n, e) ist der öffentliche Schlüssel

Falltürinformation

Wenn man $\varphi(n)$ kennt (ja!) und e und $\varphi(n)$ teilerfremd sind (ja!) gilt $m = c^d (mod\ n)$

Für d gilt dabei $d = e^{-1} (mod\ \varphi(n))$

Um aus c wieder m zu bestimmen muss man lediglich d ausrechnen - das kann man, weil man n und e passend gewählt hat. Der **geheime Schlüssel** ist also das Paar (n, d)

Die einzige Möglichkeit, als Angreifer an d zu gelangen, ist, $\varphi(n)$ zu bestimmen, also effektiv die Primfaktoren p und q des Modulus n zu berechnen - weil die Primzahlmultiplikation mit großen Primzahlen aber eine Eingwegfunktion ist, klappt das nicht.

Ablauf des RSA Verfahrens

Alice möchte, dass Bob ihr eine mit RSA verschlüsselte Mitteilung senden kann.

- Alice muss zunächst vorarbeiten: Sie wählt zufällig zwei große Primzahlen p und q und berechnet daraus den Modulus n=p·q.
- Anschließend wählt sie eine natürliche Zahl e, die teilerfremd zu φ(n) ist. Zur Erinnerung φ(n)=(p-1)·(q-1)). Die Zahlen **n und e bilden zusammen den öffentlichen Schlüssel**, den Alice öffentlich bekannt macht, also auch an Bob weitergibt. wenn ein Angreifer (Mallory) den schlüssel in die Hände bekommt ist das kein Problem.
- Alice berechnet $$d=e^{-1}(mod\; φ(n))$$. d ist der geheime Schlüssel, den sie natürlich für sich behalten muss.
- Nachdem Bob Alices öffentlichen Schlüssel hat (e,n), kann er damit seine Nachricht m, die er als Zahl betrachtet verschlüsseln. Dazu berechnet er $$c=m^e (mod\; n)$$. $$c$$ ist der Geheimtext, den er dann an Alice sendet. Die Verschlüsselung entspricht einer Modulo-Exponentiation.
- Die verschlüsselte Nachricht $$c$$ kann Alice entschlüsseln, indem sie $$c^d (mod\; n)$$ berechnet. Das Ergebnis ist der Klartext m, den Bob abgeschickt hat. Das Entschlüsseln entspricht einem Modulo-Wurzelziehen: Alice zieht die e-te Modulo-Wurzel von c, indem sie die d-te Potenz berechnet. Mallory kann d nicht ermitteln, weil er die Faktorisierung von n und damit φ(n) nicht kennt.

From:
https://www.info-bw.de/ -

Permanent link:
https://www.info-bw.de/faecher:informatik:oberstufe:kryptographie:rsaverfahren:start?rev=1648743117

Last update: **31.03.2022 16:11**