§ Kryptographie, Pseudoprimzahlen & Primzahltests

27.06.18

Ziel der Kryptographie ist es eine geheime Botschaft über einen offenen (oder unsicheren) Kanal zu versenden, sodass nur der gewünschte Empfänger die Nachricht entschlüsseln kann. Ein Problem, das seit Jahrtausenden existiert.

Notation

Klartext = die eigentliche Nachricht

Eine Verschlüsselung ändert den Klartext zu einem Geheimtext (= verschlüsselte Nachricht).

Zur Ver- bzw. Entschlüsselung wird in der Regel ein Schlüssel benötigt.

1 Die Ceasar-Chiffre

Dieses Kryptoverfahren wurde von Ceasar benutzt, um mit seinen Offizieren zu kommunizieren. Wir ordnen zunächst jedem Buchstaben eine Zahl zu:

a	b	c	...	x	y	z
0	1	2		23	24	25

Wir verschlüsseln nun unseren Kontext, indem wir jeden Buchstaben B des Klartextes einen neuen Buchstaben via der Vorschrift $C \equiv B + d \mod 26$ zu ordnen, wobei $d \in \mathbb{Z}$

(B = Buchstabe im Klartext, C = Buchstabe im Geheimtext)

Beispiel

$d = 3$ $\quad C \equiv B + 3 \mod 26$

kuchen → nxfkhg

Das Verschlusseln mit dieser Methode ist keineswegs sicher & es wird heute meist nur verwendet, um einen Text vor dem "direkten Lesen" zu schützen.

Eine direkte Verallgemeinerung ist die sogenannte affine Chiffre.

Ein Buchstabe B im Klartext wird mittels der Vorschrift $C \equiv a \cdot B + d \mod 26$ $(a,d \in \mathbb{Z})$ verschlüsselt.

Nicht jedes Paar $(a,d) \in \mathbb{Z}^2$ liefert hierbei ein Chiffrierverfahren.

Damit C wieder entschlüsselt werden kann, muss $a \in (\mathbb{Z}/m\mathbb{Z})$ ein multiplikatives Inverses haben.

Lemma 5.1.

Das obige Verfahren für $(a,d) \in \mathbb{Z}^2$ ist genau dann bijektiv, wenn $ggT(a,26) = 1$.

Auch dieses Verfahren ist nicht sicher.

Es gibt 26 Möglichkeiten für d und $\varphi(26) - 1 = 12 - 1 = 11$ Mglk.
(↑ weil $a = 1$ irrelevant ist.)

Mit einem Computer lassen sich schnell alle Möglichkeiten ausprobieren.

Ein weiteres Problem ist, dass jedem Buchstaben ein fester neuer Wert zugeordnet wird.

Im geschriebenen Text tauchen aber nicht alle Buchstaben gleich häufig auf. Dies kann man nutzen, um mittels einer Häufigkeitsanalyse den Geheimtext zu entschlüsseln.

A ~ 6,5 %, E ~ 17,4 %, Y ~ 0,03 %, U ~ 4,3 %

Wegen d. Multiplikativität von φ gilt aber $\varphi(n) = (p-1)(q-1)$

Schritt 0: (Vorbereitung)

i) Wandle den Klartext in eine Ziffernfolge um:

A = 00, B = 01, C = 02, ..., Z = 25

ii) Zerlege die so entstandene Ziffernfolge in Blöcke von gleicher gerader Länge.

Fülle den letzten Block mit Dummies, welche den Wert 26 haben

Bsp. Klartext ist MATHE, Blocklänge = 4

MA	TH	E
1200	1907	0426

Schritt 1 (Verschlüsseln)

public-key ist (e, n) mit $n = p \cdot q$ Produkt aus zwei Primzahlen & $ggT(e, \varphi(n)) = 1$

Ein Block B des Klartextes wird nun mittels der Vorschrift $C \equiv B^e \mod n$ verschlüsselt.

→ n sollte > als der Wert des maximalen Blocks sein.

Für Blöcke der Länge wäre das Z + Dummie = 2526

in der Praxis werden deutlich größere n verwendet.

Schritt 2 (Entschlüsseln)

Der private Schlüssel hat die Form (d, n), wobei d das Inverse zu e in $(\mathbb{Z}/\varphi(n)\mathbb{Z})^*$ ist. Dieses d kann aus $\varphi(n)$ berechnet werden, $\varphi(n)$ ist jedoch nicht öffentlich bekannt, da die Zerlegung $n = p \cdot q$ nicht bekannt ist.

Wir berechnen $D(c) \equiv C^d \mod n$:

Wegen $d \cdot e = 1 \in (\mathbb{Z}/m\mathbb{Z})^*$ ist $d \cdot e = 1 + k \cdot \varphi(n)$

Das RSA-Verfahren

Die affine Chiffre ist ein sog. symmetrisches Verschlüsselungsverfahren,
d.h. jeder der verschlüsseln kann, kann auch wieder entschlüsseln.
Sender und Empfänger müssen sich also zunächst auf einen gemeinsamen Schlüssel verständigen. Im Zeitalter des Internets ist dies wenig praktikabel.
Um dies zu umgehen benutzt man unsymmetrische Verschlüsselungsverfahren sogenannte "public-key-Kryptosysteme"
In einem solchen Verschlüsselungsverfahren werden 2 verschiedene Schlüssel benutzt.

- Einen öffentlichen Schlüssel (= public-key)
- Einen privaten Schlüssel (= private-key)

Nur wer den privaten Schlüsseln kennt, kann entschlüsseln.
Zum verschlüsseln genügt hingegen d. öffentliche Schlüssel.
Im folgenden werden wir das RSA-Verfahren besprechen, welches 1976 von Rives, Shamir & Adlemann patentiert wurde.

Das RSA-Verfahren basiert auf modularen Potenzieren (vgl. Übung 11)
Der öffentliche Schlüssel besteht aus zwei Teilen

- einem Exponenten e
- einem Modulus n, der ein Produkt aus zwei (großen) unterschiedlichen Primzahlen ist, also $n = pq$

Zudem soll gelten, dass $ggT(e, \varphi(n)) = 1$
Die Zerlegung $n = p \cdot q$ ist dabei nicht öffentlich bekannt, sondern nur n.

Nach dem Satz von Euler ist

$B^{\varphi(n)} \equiv 1 \bmod r$, falls B und n teilerfremd sind, was sehr wahrscheinlich ist, da n ein Produkt aus zwei Primzahlen ist. Also $D(C) \equiv C^d \equiv (B^e)^d \equiv B^{e \cdot d} \equiv B^{1+k \cdot \varphi(n)}$

$$\equiv B \cdot \underbrace{(B^{\varphi(n)})^k}_{\equiv 1 \bmod n} \equiv B \bmod n$$

Also ist der verschlüsselte Buchstabe C entschlüsselt.

Beispiel 5.2

$n = 3127 = 53 \cdot 59$ $\quad e = 17$

MATHE $\hat{=}$ 1200 1907 0426

$(1200)^{17} \equiv 2565 \bmod n$

$(1907)^{17} \equiv 1377 \bmod n$

$(0426)^{17} = (426)^{17} \equiv 1222 \bmod n$

↝ Geheimtext ist 2565 1377 1222

Der private Schlüssel ist $(d = 2129, n)$ $\quad (\varphi(n) = 3016 = 52 \cdot 58)$

$(2565)^d \equiv 1200 \bmod n$

$(1377)^d \equiv 1907 \bmod n$

$(1222)^d \equiv 0426 \bmod n$

Das Verfahren funktioniert, da es leicht ist Schlüssel zu bauen & zu ver- bzw. entschlüsseln, aber sehr schwer zu knacken ist.

Um den Code zu knacken, muss man $d = \bar{e}^1 \in (\mathbb{Z}/\varphi(n)\mathbb{Z})^*$ berechnen. Das Problem hierbei ist es $\varphi(n)$ zu berechnen.

Lemma 5.3

Sei $n = p \cdot q$ eine RSA-Zahl (also Produkt aus zwei unters. Primzahlen p, q) Die Berechnung von $\varphi(n)$ ist äquivalent zur Berechnung der Zerlegung $n = p \cdot q$

Beweis:

Kennt man die Zerlegung $n = p \cdot q$, so ist $\varphi(n) = \varphi(p) \cdot \varphi(q)$
$= (p-1) \cdot (q-1)$.

Sei umgekehrt $\varphi(n)$ bekannt. Wir kennen n und wissen, dass $\varphi(n) = (p-1) \cdot (q-1)$, da n eine RSA-Zahl ist.

Wir haben:

$$n+1-\varphi(n) = p \cdot q + 1 - (p-1)(q-1) = p+q \quad \&$$

$$\sqrt{(p+q)^2 - 4n} = \sqrt{p^2+2pq+q^2-4pq} = \sqrt{(p-q)^2} = |p-q|$$

OE $p > q$. Dann ist $|p-q| = p-q$

$p = \frac{1}{2} \cdot [(p+q)+(p-q)]$, $q = \frac{1}{2}[(p+q)-(p-q)]$ ☒

Das Faktorisieren großer RSA-Zahlen ist extrem schwierig. Die Firma, der das Patent am RSA-Verfahren gehört, hatte vor 7-8 Jahren Preisgelder ausgesetzt, um große RSA-Zahlen zu faktorisieren.