§ 3 Kryptologie

Ziel der Kryptologie:
Konstruktion von Verschlüsselungsvorschriften, die „leicht" durchzuführen sind, wobei aber die inverse Entschlüsselung - ohne weitere Kenntnisse, die nur der Empfänger hat - „schwer" sein soll.

Beispiel einer Verschlüsselungsfunktion:
Für festes t mit $0 \leq t \leq 25$ wird jeder Buchstabe des gewöhnlichen Alphabets um t Stellen nach rechts (bzw. $26-t$ Stellen nach links) verschoben.
Für $t = 4$ ergibt sich etwa

Klartext $\longrightarrow$ Geheimtext
ZAUN DEYR

Annahme:
Der Unbefugte weiß, dass nach diesem Algorithmus verschlüsselt wird, aber nur der Empfänger kennt von vornherein den Wert t.

Im allgemeinen ist es aber für den Unbefugten leicht, t zu ermitteln:
Es gibt in der Regel nur eine Möglichkeit, ein sinnvolles deutsches Wort (oder einen deutschen Text) zu erhalten.

<u>Konventionen 3.1:</u>

Gegeben seien zwei Mengen $\mathcal{A}$ und $\mathcal{B}$ mit mindestens 2, aber höchstens endlich vielen Elementen, genannt <u>Alphabete</u>.

Zum Beispiel kann

$$\mathcal{A} = \{A, B, C, \dots, Z\}$$

das gewöhnliche Alphabet in Block-Buchstaben sein und

$$\mathcal{B} = \mathcal{A} \text{ oder } \mathcal{B} = \{ k \in \mathbb{Z} \mid 0 \le k \le 9 \}.$$

Die Elemente von $\mathcal{A}$ und $\mathcal{B}$ heißen <u>Buchstaben</u>.

Wir setzen

$$(*) \qquad \mathcal{A}^* := \{ (A_1, \dots, A_n) \mid n \ge 1,\ A_i \in \mathcal{A} \text{ für } 1 \le i \le n \}$$

$$= \dot{\bigcup_{n \ge 1}} \mathcal{A}^n$$

und definieren $\mathcal{B}^*$ entsprechend.

$\mathcal{A}^*$ ist also das System aller endlichen Folgen aus $\mathcal{A}$.

Die Elemente aus $\mathcal{A}^*$ bzw. $\mathcal{B}^*$ heißen <u>Texte</u> über dem Alphabet $\mathcal{A}$ bzw. $\mathcal{B}$.

<u>Definition 3.2:</u>

i) Eine <u>Chiffrierung</u> oder <u>Verschlüsselungsfunktion über $\mathcal{A}$ mit Werten in $\mathcal{B}^*$</u> ist eine injektive Abbildung $f: \mathcal{A}^* \to \mathcal{B}^*$.

Für einen Text $(A_1, \dots, A_n) \in \mathcal{A}^*$ heißt $f(A_1, \dots, A_n) \in \mathcal{B}^*$ der verschlüsselte – oder <u>chiffrierte</u> – Text.

ii) Eine Chiffrierung $f: \mathcal{A}^* \to \mathcal{B}^*$ heißt eine <u>Stromchiffrierung</u>, wenn sie <u>zeichenweise</u> durchgeführt wird; das heißt, für alle $(A_1, \ldots, A_n) \in \mathcal{A}^*$ gilt:

$$f(A_1, \ldots, A_n) = (f(A_1) \ldots f(A_n)).$$

<u>Bemerkung 3.3:</u>

Manchmal ist die injektive Abbildung f nur auf einer Teilmenge M von $\mathcal{A}^*$ definiert, die eine <u>Sprache</u> über dem Alphabet $\mathcal{A}$ bezeichnet. Dabei heißt M der <u>Klartextraum</u>, und die Elemente von M heißen <u>Klartexte</u> oder <u>sinnvolle Texte</u>. Die Elemente der Bildmenge $f(M)$ werden <u>Geheimtexte</u> - oder <u>Kryptogramme</u> - genannt.

Üblicherweise wird f aber auf ganz $\mathcal{A}^*$ definiert, auch wenn nur Texte aus M chiffriert werden sollen.

<u>Beispiel 3.4:</u>

Sei $\mathcal{A} = \{A, B, C, \ldots, Z\}$ das gewöhnliche Alphabet und $\mathcal{B} = \{k \in \mathbb{Z} \mid 0 \leq k \leq 9\}$.

Auf $\mathcal{A} = \mathcal{A}^1$ wird f durch folgende Tabelle bestimmt:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Für $0 \leq i \leq 25$ wird also dem $(i+1)$-ten Buchstaben die zweistellige Dezimaldarstellung der Zahl i zugeordnet.

Das heißt insbesondere:

Für $0 \leq i \leq 9$ beginnt die Dezimaldarstellung mit der Ziffer 0.

Auf $\mathcal{A}^*$ wird f nun so definiert, dass f eine Stromchiffrierung ist.

Für $(A_1, \dots, A_n) \in \mathcal{A}^n$, $n \geq 2$, setzen wir also:

$$f(A_1 \dots A_n) = f(A_1) f(A_2) \dots f(A_n) \in \mathcal{B}^{2n}.$$

Weil jeder Buchstabe aus $\mathcal{A}$ eineindeutig auf ein Element aus $\mathcal{B}^2$ abgebildet wird, ist f auf ganz $\mathcal{A}^*$ injektiv.

Warnung:

Wird die Stromchiffrierung f im letzten Beispiel so modifiziert, dass bei den Bildern der Buch=staben A-J jeweils die führende 0 ignoriert wird, so ist f nicht injektiv; denn es folgte:

$$f(BB) = f(B) f(B) = 11 = f(L).$$

Das Element 11 ließe sich also nicht eindeutig entschlüsseln.

Definition 3.5:
Sei $f: \mathcal{A}^* \to \mathcal{B}^*$ eine Chiffrierung und $\tilde{\mathcal{B}} := f(\mathcal{A}^*)$ der Bildraum von f. Die zugehörige - bijektive - Umkehrabbildung $f^{-1}: \tilde{\mathcal{B}} \to \mathcal{A}^*$ heißt Dechiffrierung. Das zugehörige Kryptosystem besteht aus der Chiffrierung f und der inversen Dechiffrierung f^{-1}.

Skizze

$$\mathcal{A}^* \xrightarrow{f} \tilde{\mathcal{B}} \xrightarrow{f^{-1}} \mathcal{A}^*$$

Definition 3.6, Die Skytala-Verschlüsselung:
Ein Text wird nach folgender Vorschrift chiffriert bzw. dechiffriert:

Schlüssel: $n \in \mathbb{N}$

Chiffrieren: Schreibe den Klartext zeilenweise in ein Schema mit genau n Zeilen, in dem jede Spalte n oder $n-1$ Buchstaben aufweist.
Man erhält den Geheimtext, indem der Text spaltenweise gelesen wird.

Dechiffrieren: Schreibe den Geheimtext spaltenweise in ein Schema mit genau n Zeilen.
Man erhält den Klartext, indem man zeilenweise liest.

Bemerkung 3.7, Geometrische Interpretation:

Wickele ein schmales Band spiralförmig um einen Zylinder, und schreibe der Zylinderlänge nach eine Nachricht auf das Band.
u ist - in Bezug auf die Anzahl der Buchstaben - der Umfang des Zylinders. Nach Abwickeln des Bandes erhält man den Geheimtext.

Beispiele:

i) Wir chiffrieren - für $u = 3$ - das Wort

STEUERSCHAETZER

und erhalten das Schema

STEUE
RSCHA
ETZER

Spaltenweises Lesen liefert den Geheimtext

SRETSTECZUHEEAR

ii) Gegeben sei der Geheimtext

NSAEUKCRSNK

Zum Entschlüsseln können verschiedene mögliche Umfänge u ausgetestet werden. Ordnen wir den Text in $u = 4$ Zeilen an, so erhalten wir

NUS
SKN
ACK
ER

Das gesuchte Wort ist also:

NUSSKNACKER

<u>Definition 3.8:</u>
Eine bijektive Funktion $f: M_1 \to M_2$ heißt eine <u>Einwegfunktion</u>, wenn für $c \in M_2$ die Ermittlung von $f^{-1}(c)$ - ohne zusätzliche Kenntnisse - „schwer" ist.

<u>Bemerkung 3.9:</u>
Für die heutigen Anwendungen der Kryptologie ist weniger gravierend, dass Definition 3.8 keine exakte mathematische Definition ist.
Wesentlich ist: Die Berechnung der Bilder unter f ist erheblich einfacher als die Berechnung der Urbilder.
Häufig wird verlangt: Zum jetzigen Zeitpunkt ist <u>kein polynomialer Algorithmus</u> zur Berechnung der Urbilder <u>bekannt</u>.

<u>Definition 3.10:</u>
Sei $\mathcal{A}_0 \subseteq \mathcal{A}^*$, und sei K eine Menge von Personen. Sei $(E_T)_{T \in K}$ eine Familie von Abbildungen von $\mathcal{A}_0$ nach $\mathcal{B}^*$, genannt die <u>öffentlichen Schlüssel-Funktionen</u>, und $(D_T)_{T \in K}$ sei eine Familie von Abbildungen von $\mathcal{B}^*$ nach $\mathcal{A}^*$, genannt die <u>geheimen Schlüssel-Funktionen</u>.
Das System $(\mathcal{A}_0, \mathcal{B}^*, (E_T)_{T \in K}, (D_T)_{T \in K})$ heißt ein <u>Public-Key-Verschlüsselungssystem</u>, falls gilt:

(I) Jede Funktion E_T, $T \in K$, ist eine Einwegfunktion.

(II) Für alle $T \in K$ und alle $m \in \mathcal{A}_0$ gilt:

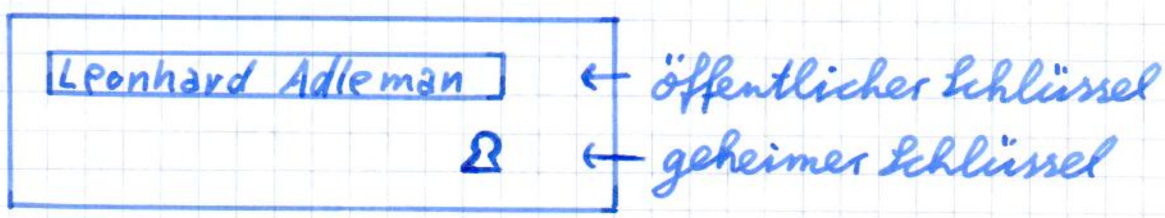
$$D_T(E_T(m)) = m.$$

<u>Bemerkungen 3.11:</u>

i) Die öffentlichen Schlüssel-Funktionen - oder kurz öffentlichen Schlüssel - dienen zum Chiffrieren und sind allgemein bekannt, während die geheimen - oder <u>privaten</u> - Schlüssel zum Dechiffrieren dienen und nur dem jeweiligen Besitzer bekannt sind.

ii) Um einer festen Person $T \in K$ eine geheime Nachricht m zu übermitteln, kann ihr die verschlüsselte Nachricht $E_T(m)$ gesendet werden, die ja - nach (I) und (II) - nur von T selbst wieder „leicht" zu entschlüsseln ist.

iii) Die Rolle der - öffentlichen und geheimen - Schlüssel kann durch folgendes Bild eines Briefkastens illustriert werden:



Der öffentliche Schlüssel ist das Namensschild mit der Öffnung. Nur der Besitzer kann das Fach mit seinem Schlüssel öffnen.

Der RSA-Algorithmus 3.12, nach Rivest, Shamir, Adleman (1977):

Schritt I. Jede Person wählt zwei verschiedene - und große - Primzahlen p und q und berechnet $n = p \cdot q$.
Ferner berechnet sie $\varphi(n) = (p-1)\cdot(q-1)$.
Schließlich wählt sie eine Zahl e mit $1 \leq e < \varphi(n)$, die zu $\varphi(n)$ teilerfremd ist, und berechnet d mit $1 \leq d < \varphi(n)$ und

$$e \cdot d \equiv 1 \bmod \varphi(n).$$

Schritt II. Als öffentlichen Schlüssel gibt sie das Paar (e, n) bekannt; p und q bleiben geheim.
Der private Schlüssel ist d.

Schritt III. Wir setzen

$$\mathcal{C}_n := \{r \in \mathbb{Z} \mid 0 \leq r < n\}.$$

Ein Text T über einem zugrunde liegenden Alphabet wird mittels einer Stromchiffrierung als ein Element aus $\mathcal{C}_n^*$ - also einer Folge aus $\mathcal{C}_n$ - dargestellt.

Schritt IV. Die Verschlüsselung von Elementen aus $\mathcal{C}_n$ erfolgt nach der Vorschrift
$f_e : \mathcal{C}_n \to \mathcal{C}_n$, festgelegt durch

$$f_e(r) \equiv r^e \bmod n.$$

Bemerkungen 3.13:

i) Die <u>Entschlüsselung</u> $f_d: C_n \to C_n$ ist festgelegt durch

$$f_d(r) \equiv r^d \mod n.$$

ii) Wegen $e \cdot d \equiv 1 \mod \varphi(n)$ gilt:

$$k := \frac{e \cdot d - 1}{\varphi(n)} = \frac{e \cdot d - 1}{(p-1)\cdot(q-1)} \in \mathbb{N}.$$

Damit liefert Satz 2.25 für alle $m \in C_n$:

$$f_d(f_e(m)) \equiv (m^e)^d \equiv m^{e \cdot d} \equiv m^{k\cdot(p-1)\cdot(q-1)+1}$$
$$\equiv m \mod n.$$

Wegen $m, f_d(f_e(m)) \in C_n$ bedeutet das:

$$f_d(f_e(m)) = m.$$

Das heißt: Bedingung (II) in Definition 3.10 ist erfüllt.

iii) Für $m \in C_n$ ist die Berechnung von $f_e(m)$ einfach.

iv) Die -prinzipiell analoge- Berechnung von $f_d(r)$ für $r \in C_n$ ist nur einfach, <u>wenn</u> der private Schlüssel d bekannt ist.
d ließe sich - etwa mittels des Euklidischen Algorithmus - aus der Kongruenz $e \cdot d \equiv 1 \mod \varphi(n)$ berechnen, <u>wenn</u> $\varphi(n) = (p-1)\cdot(q-1)$ bekannt wäre.
Wäre neben n auch $\varphi(n)$ öffentlich bekannt, so ließen sich p und q aus den Gleichungen

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

berechnen.

v) Es ist kein schneller Algorithmus zur Faktorisierung großer Zahlen bekannt.

Resümierend können wir sagen, dass auch Bedingung (I) in Definition 3.10 erfüllt ist.

Das bedeutet:

Nach unserem jetzigen Kenntnisstand ist das RSA-System ein sicheres Public-Key-Verschlüsselungssystem.

<u>Beispiel 3.14:</u>

Wir schreiben

$A \hat{=} 01,\ B \hat{=} 02, \ldots, Z \hat{=} 26$; Leerzeichen $\hat{=} 00$,

$\mathcal{A} = \{00, 01, 02, \ldots, 26\}$.

Weiter sei

$\mathcal{B} = \{n_1 n_2 n_3 n_4 \mid 0 \leq n_i \leq 9$ für $1 \leq i \leq 4\}$.

Dabei bedeutet, wie üblich, $n_1 n_2 n_3 n_4$ die Zahl

$$1000 \cdot n_1 + 100 \cdot n_2 + 10 \cdot n_3 + n_4 .$$

In dem Text

KOMME MORGEN ZURUECK

werden zunächst aufeinanderfolgende Bigramme (das sind Blöcke von zwei Buchstaben) verschlüsselt; damit erhalten wir folgende Folge von 4-Blöcken:

$$\begin{array}{l} 1115 \mid 1313 \mid 0500 \mid 1315 \mid 1807 \mid \\ 0514 \mid 0026 \mid 2118 \mid 2105 \mid 0311 \end{array} \qquad (*)$$

Wir wählen nun die Primzahlen $p = 47$, $q = 59$ und erhalten:

$$n = 47 \cdot 59 = 2773,$$

$$\varphi(n) = 46 \cdot 58 = 2668 \; .$$

Für $e = 17 = 2^4 + 1$ wird der Text in $(*)$ nun vermöge f_{17} mod 2773 verschlüsselt, indem jeder 4-Block mit 17 mod 2773 potenziert wird:

$$1379 | 2395 | 1655 | 0422 | 0482 |$$

$$1643 | 1445 | 0848 | 0747 | 2676 \qquad (**)$$

Beispielsweise erhalten wir modulo 2773:

$$1115^2 \equiv 921$$

$$1115^4 \equiv 921^2 \equiv 2476,$$

$$1115^8 \equiv 2476^2 \equiv 2246,$$

$$1115^{16} \equiv 2246^2 \equiv 429,$$

$$1115^{17} \equiv 429 \cdot 1115 \equiv 1379.$$

Die Verschlüsselung ist injektiv, weil alle möglichen 4-Blöcke - insbesondere die in $(*)$ - unterhalb von 2773 liegen.

Bemerkung 3.15,
siehe auch Beispiel 4.12 vom WS 2015/16:

Für $n \in \mathbb{N}$ mit $n \geq 2$ und $m \in \mathbb{Z}$ ist

$$m + n\cdot\mathbb{Z} := \{m + n\cdot k \mid k \in \mathbb{Z}\} = \{a \in \mathbb{Z} \mid a \equiv m \bmod n\}.$$

Ferner ist der Restklassenring modulo n die Menge

$$\mathbb{Z}/n\cdot\mathbb{Z} := \{m + n\cdot\mathbb{Z} \mid 0 \leq m \leq n-1\}.$$

Schreiben wir kurz $\overline{m} := m + n\cdot\mathbb{Z}$ für $m \in \mathbb{Z}$, so sind die Addition und die Multiplikation in $\mathbb{Z}/n\cdot\mathbb{Z}$ gegeben durch:

$$\overline{m} + \overline{l} := \overline{m+l} \quad , \quad \overline{m}\cdot\overline{l} := \overline{m\cdot l} \quad \text{für } m, l \in \mathbb{Z}.$$

Beim Übergang von $\mathbb{Z}$ zu $\mathbb{Z}/n\cdot\mathbb{Z}$ werden zwei Zahlen, deren Differenz durch n teilbar ist, identifiziert.

Das bedeutet:
Das Rechnen in $\mathbb{Z}/n\cdot\mathbb{Z}$ ist gleichbedeutend mit dem Rechnen modulo n.

Definition 3.16:
Sei p eine ungerade Primzahl, und sei $2 \leq g \leq p-1$.
i) Die Funktion $E_g : \{1, \dots, p-1\} \to \mathbb{Z}/p\cdot\mathbb{Z}$,
definiert durch

$$E_g(x) := \overline{g}^{\,x} \qquad \text{mit } \overline{g} := g + p\cdot\mathbb{Z}$$

heißt die Exponentialfunktion modulo p zur Basis g.

ii) Ist umgekehrt $\overline{y} = y + p \cdot \mathbb{Z} \in \mathbb{Z}/p \cdot \mathbb{Z}$ gegeben mit $p \nmid y$, so heißt jede Zahl $x \in \mathbb{Z}$ mit $\overline{g}^x = \overline{y}$ <u>ein Diskreter Logarithmus von y modulo p zur Basis g</u>.

<u>Bemerkungen 3.17:</u>

i) Für p und g wie in Definition 3.16 gibt es nicht unbedingt zu jedem $y \in \mathbb{Z}$ mit $p \nmid y$ einen Diskreten Logarithmus von y modulo p zur Basis g.
Allerdings kann – bei vorgegebener ungerader Primzahl p – die Zahl $g \in \{2, \dots, p-1\}$ so <u>gewählt</u> werden, dass zu dieser Basis g all diese Logarithmen existieren.
Eine Basis g mit dieser Eigenschaft heißt auch <u>Primitivwurzel modulo p</u>.

ii) Nach obigen Ausführungen ist die Berechnung von Werten von Exponential=funktionen modulo p einfach, nicht aber die Berechnung von Diskreten Logarithmen.