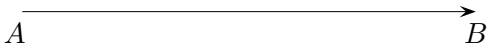
RSA-Verschlüsselung



A möchte B eine Zahl T verschlüsselt zusenden.
Denkbar wäre $T + 17$.
Damit B die Nachricht entschlüsseln kann, muss ein Kontakt („Du musst 17 subtrahieren.“) zwischen A und B stattgefunden haben.

Kann es ein Verschlüsselungsverfahren geben, das ohne einen vorherigen Kontakt auskommt?
B könnte im Internet bekanntgeben, dass von einer Zahl, die ihm zugesandt werden soll, vorher das Quadrat zu gebilden ist. B wüsste die Umkehroperation, jedoch alle Anderen auch.

B konnte versucht sein, eine Funktion zu verwenden, deren Umkehrfunktion kompliziert ist.
Der effektivere Weg ist jedoch, eine Funktion zu basteln, deren Umkehrfunktion (Entschlüsselung) nur mit dem Konstruktionswissen in kurzer Zeit ausgeführt werden kann, ansonsten es Jahre dauern würde.

Tatsächlich gelingt es B mit dem Produkt $N = p \cdot q$ zweier Primzahlen (jeweils 100stellig) und einer hiermit ermittelten Zahl e ein einfaches Verfahren für die

$$\begin{aligned} \text{Verschlüsselung} \qquad & G = T^e \mod N \\ \text{und Endschlüsselung} \qquad & T = G^d \mod N \end{aligned}$$

zu entwickeln, $\mod N$ ist der Rest bei Division durch N. Die Potenz ist daher kleiner als N.
B veröffentlicht N und e und das Verschlüsselungsverfahren $G = T^e \mod N$.
Die beiden Primzahlen und die aus der Konstruktion sich ergebende Zahl d werden nicht verraten.

Zum Verständnis sind elementare Kenntnisse der Zahlentheorie (Rechnen in Restklassen, eulersche φ-Funktion, Satz von Euler, erweiterter euklidischer Algorithmus) erforderlich.

Wahl von e: $1 < e < \varphi(N) = (p-1) \cdot (q-1)$ und $\mathrm{ggT}(e, \varphi(N)) = 1$

Wahl von d: $e \cdot d = 1 \mod \varphi(N)$, d. h. es ist die Gleichung $e \cdot d + \varphi(N) \cdot q = 1$ zu lösen.

Um die Verschlüsselung zu knacken müsste, um d zu ermitteln, das N in seine zwei Primfaktoren zerlegt werden. Nach heutigem Wissensstand ist dies für große Zahlen in keiner vertretbaren Zeit möglich.

1978 entwickelten Rivest, Shamir und Adleman die dargestellte RSA-Verschlüsselung, Diffie und Hellman zuvor die Theorie. Mit einer kleinen Abänderung kann das Verfahren auch für digitale Signaturen verwendet werden, d. h. B weiß dann genau, dass die Nachricht von A stammt.

Asymmetrische Verschlüsselung

Derjenige, der eine verschlüsselte Nachricht empfangen will, sendet eine Kiste mit offenem Vorhängeschloss an den Sender. Dieser legt die Nachricht in die Kiste und schließt das Schloss. Der Schlüssel bleibt beim Empfänger, sodass nur er die Kiste wieder öffnen kann. Digital gelingt das Szenario wie folgt: Aus zwei großen Primzahlen wird ein Produkt gebildet. Die beiden Primzahlen kennt aber nur der Empfänger der Nachricht, sie sind sozusagen der Schlüssel. Das Produkt ist das Vorhängeschloss, es wird an den Sender geschickt. Mithilfe eines Algorithmus verschlüsselt dieser mit der erhaltenen Zahl die Nachricht. Entschlüsselt werden kann sie aber nur mithilfe der beiden Faktoren, nicht durch das Produkt der Faktoren.

AES-Verschlüsselung

ADVANCED ENCRYPTION STANDARD 2001

2A			
		FF	

$\underbrace{1011}_{\text{B}}\underbrace{0101}_{5} = \text{B5}$

1 Byte sind 8 Bit. Je 4 Bit können zu einer hexadezimalen Ziffer zusammengefasst werden.

Die zu verschlüsselnden Daten liegen jeweils in einer 4×4-Matrix vor.
Diese Datenblöcke beinhalten 16 Byte.
Ein (geheimer) 128-Bit-Schlüssel legt fest, wie der Klartext schrittweise durch eine Folge von

a) bitweisen XOR-Verknüpfungen mit Tabellen-Zahlen, die mit dem Schlüssel generiert wurden,
b) Ersetzungen,
c) zyklischen Spaltenverschiebungen,
d) spaltenweiser Vermischungen
e) und spezieller Rechenoperationen

in einen Geheimtext umgewandelt wird.

$2^8 = 256$ Byte-Werte sind möglich.
Bemerkenswert sind die verwendeten Rechenoperationen auf diesen Werten.
Hierbei wird auf eine algebraische Struktur (endl. Körper, 2. Semester) zurückgegriffen,
in der nach den uns bekannten Rechengesetzen addiert und multipliziert werden kann.
Ansonsten haben diese Rechenoperationen mit den Verknüpfungen der reellen Zahlen nur die Bezeichnungen gemeinsam.

Die Restklassen modulo p (p Primzahl) bilden einen endl. Körper mit p Elementen.
Für weitere Körperkonstruktionen werden Polynome verwendet. So auch hier.