Im Folgenden lernst du ein Verfahren kennen, wie es heute im täglichen Leben zum Einsatz kommt, z.B. bei Transaktionen mit Kreditkarten u.ä.

Das RSA-Verfahren
(nach den Entwicklern **R**ivest, **S**hamir und **A**dleman)

Das RSA-Verfahren wurde in den 1970er-Jahren entwickelt. Nachdem es 1977 eigentlich bereits fertig war, dauerte es immer noch bis 1983, bis es zum Patent angemeldet wurde. Ver- und entschlüsselt wird mit modularer Potenzierung, als Einwegfunktion wird das modulare Multiplizieren benutzt.

RSA ist ein asymmetrisches Verfahren[1] und arbeitet folgendermaßen:

Die beiden Freunde Alice und Bob wollen sich abhörsicher per RSA-Verfahren unterhalten:

1. **Alice erzeugt ihren geheimen („privaten") Schlüssel:**
   Dieser wird folgendermaßen bestimmt: Sie wählt zwei Primzahlen p und q und verschafft sich eine dritte Zahl e, die mit p und q auf bestimmte Weise zusammenhängt.

   Im Detail: **Alice wählt p = 11 und q = 23.**

   Nun die Zahl e: Bedingung an e ist, dass e teilerfremd zur Zahl $(p - 1) \cdot (q - 1)$ ist und im Bereich $1 < e < (p - 1) \cdot (q - 1)$ liegt, hier also:

   e ist teilerfremd zu (11-1) · (23-1) = 10·22 = 220 und **1 < e < 220.**

   Übersichtlicher wird die Situation, wenn man sich von $(p - 1) \cdot (q - 1)$ die Primfaktorzerlegung (PFZ) anschaut: $220 = 2^2 \cdot 5 \cdot 11$. Also *wählt* sich Alice eine zu $2^2 \cdot 5 \cdot 11$ teilerfremde Zahl im Bereich $1 < e < 220$, z.B. eine Primzahl, die in $2^2 \cdot 5 \cdot 11$ nicht vorkommt:

   z.B. e = 13.

   Ihren geheimen Schlüssel d erzeugt Alice nach der Formel

   1 = (e·d) mod (p-1)·(q-1), also im Beispiel **1 = (13·d) mod 220**

   Für d = 17 ist dies erfüllt. Prüfe das per Probe selbst nach.
   Bem: Wie bestimmt man d allgemein? Kommt dir dieser Ansatz zur Bestimmung von d bekannt vor? Durchforsche deinen Aufschrieb bei „Verschlüsseln mittels Multiplikation"

   Der geheime Schlüssel von Alice lautet (d; N) = (17; 253).
   Die Zahl N ist das sog. „RSA-Modul" und berechnet sich als $N = p \cdot q = 11 \cdot 23 = 253$

1 Kennst du den Begriff „asymmetrische Verschlüsselung" schon? Wenn nicht, dann lernst du ihn noch in diesem Jahr im Informatik-Unterricht kennen.

2. **Alice erzeugt ihren öffentlichen Schlüssel:**
   Dieser besteht aus den beiden Zahlen e und N aus Abschnitt 1.

   Der öffentliche Schlüssel von Alice lautet (e ; N) = (13 ; 253).

3. Nun möchte Bob eine liebe Nachricht an Alice schicken. Er wählt dazu (wie in englischsprachigen Ländern üblich) das „X“ als Symbol für einen Kuss, dessen ASCII-Übersetzung „88“ lautet. Diese Botschaft möchte er nun verschlüsseln und an Alice schicken. Er kennt Alice' öffentlichen Schlüssel und verschlüsselt damit nun folgendermaßen:

   Bob's Verschlüsselung: $S = B^e \bmod N$

   Also $S = 88^{13} \bmod 253$.

   Berechne Bobs Geheimnachricht: _____

   Bob schickt nun seine Geheimnachricht an Alice.

4. Alice erhält also die Zahl ____ als Botschaft von Bob. Sie entschlüsselt nun mit der Zahl d = 17 ihres privaten Schlüssels auf prinzipiell die selbe Art, wie Bob verschlüsselt hat:

   Alice' Entschlüsselung: $B = S^d \bmod N$

   Also: B = _____ mod 253 = _____.

Aufgabe:
Vergleiche die Formeln der Ver- und Entschlüsselung: Bei gleicher Struktur unterscheiden sich die Inhalte der Formeln. Formuliere hier aus, wie:

_____

_____

_____

_____

Wechselseitige Kommunikation

Möchte nun Alice auf Bobs Nachricht antworten, so muss das Vorgehen zur Schlüsselerzeugung von Bob gerade noch einmal vorgenommen werden: Bob muss einen geheimen und einen privaten Schlüssel erzeugen, damit Alice ihm antworten und ebenso verfahren kann wie er. Führe hier nochmals das Procedere nach der Anleitung für Alice (s. oben) an einem Beispiel mit nicht zu großen Zahlen für Bob durch:

X Wahl zweier _____: p =_____ q = _____

X _____

X _____

X _____

X _____

X _____

Probiere es aus:

1. *Suche dir eineN PartnerIn.*
2. *Legt (jedeR für sich!) eure öffentlichen Schlüssel fest, tauscht sie aus.*
3. *Erstellt eure geheimenSchlüssel*
4. *Denkt euch eine Botschaft aus und schickt sie euch RSA-verschlüsselt*
5. *Fangt eine Botschaft einer anderen Gruppe ab und versucht sie zu knacken! (Bem.: die öffentlichen Schlüssel dürft ihr dabei verwenden. Sie sind ja „öffentlich“!)*

Hier noch ein kleines Ablaufschema zur Kommunikation:

Beide (Alice und Bob) sind einmal Sender und ein anderes Mal Empfänger. Hier ist eine Übersicht, was man jeweils als Sender bzw. Empfänger zu tun hat:

Bem.: eine schöne Onlineanimation dieses Verfahrens findest du bei matheonline.at (aufgerufen am 12.05.2020): *https://www.mathe-online.at/materialien/Franz.Embacher/files/RSA/*
Bitte beachten: zur Verwendung ist der Flash-Player erforderlich.

Empfänger	**Sender**
Vorbereitung der Kommunikation: *Wahl von p und q:* p = _____ ; q = _____ *Berechnung:* N = p · q = _____ sowie m = (p-1) · (q-1) =_____ *Wahl e:* 1 < e < m mit Bed.: e teilerfremd zu m: e = _____ Berechnung von d nach der Formel 1 = (e·d) mod (p-1)·(q-1) ; d = _____	
Geheimer Schlüssel von Alice: d = _____ (bleibt bei Alice) Öffentlicher Schlüssel von Alice: (N, e) = (_____ ; _____) → Bob	Bob bekommt den öffentlichen Schlüssel von Alice (N, e)
	Verschlüsselt seine Nachricht B = _____ und erhält den Geheimtext S mit der Formel $S = B^e \bmod N$ = _____ = _____
Erhält S von Bob	← sendet S an Alice
Entschlüsselt S mittels der Formel $B = S^d \bmod N$ = _____ = _____	