© D. Kruse, BBS II Leer bearbeitet von J. Rau, 2021

Das RSA-Verfahren

I. Alice erzeugt zuerst Ihren privaten Schlüssel

Sie wählt **zwei Primzahlen**, z. B. $p = 17$ und $q = 11$.
Diese beiden Zahlen muss Alice geheim halten!
Nun wählt Alice noch eine weitere **Zahl *e***. z.B. $e = 7$.
e und **(p-1) · (q-1)** müssen teilerfremd sein und kleiner als **p · q**

Den **privaten Schlüssel *d*** berechnet Sie dann aus ***p, q*** und ***e*** mit der Formel

$(e \cdot d)\ mod\ (p - 1) \cdot (q - 1) = 1$

Mit den eingesetzten Werten für e, p und q lautet die Gleichung:

$(7 \cdot d)\ mod\ ((17 - 1) \cdot (11 - 1)) = 1$

$(7 \cdot d)\ mod\ ((16) \cdot (10)) = 1$

$(7 \cdot d)\ mod\ 160 = 1$

Für ***d* = 23** stimmt die Gleichung: $1 = (7 \cdot 23)\ mod\ 160 = 161\ mod\ 160$

II. Alice erzeugt dann ihren öffentlichen Schlüssel, er besteht aus zwei Zahlen. Als erste Zahl verwendet Alice ***e = 7***. Die zweite Zahl ist das Produkt ***N= p · q*** *N= 187.* Die Zahlen ***N* und *e*** sind der **öffentliche Schlüssel.**

III. Die zu verschlüsselnde Nachricht wird in eine *Zahl M* umgewandelt. Das kann mit dem ASCII-Code geschehen. Nehmen wir an, Bob möchte Alice den Buchstaben **X** als symbolischen Kuss schicken. Das X hat im ASCII-Code den Dezimalwert 88. Daraus folgt ***M = 88***.

IV. Jetzt kann Bob die *Zahl M* verschlüsseln und erzeugt die *verschlüsselte Nachricht C*. Die Verschlüsselung von *M* zu *C* erfolgt mit der Formel

$C = M^{e}$ mod N

Bob erhielt $e = 7$ und $N = 187$ von Alice.
Bob rechnet also: **$C = 88^{7}$ mod *187***
Mit der wissenschaftlichen Ansicht des Windows-TR erhält man C =**11**

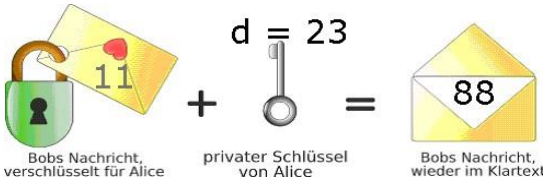
Bob schickt die verschlüsselte Nachricht *C* = 11 an Alice.

V. Alice entschlüsselt die empfangene Nachricht *C*. Dazu benötigt sie den privaten Schlüssel $d = 23$ und den öffentlichen Teil Schlüssels $N = 187$.

$M = C^{d}$ mod N

Die Berechnung der Originalnachricht: **$M = 11^{23}$** mod 187 → M = 88 → ASCII-Code=X

Hätte ihr Vater den Brief abgefangen, hätte er die Zahl 11 gelesen.



© D. Kruse, BBS II Leer bearbeitet von J. Rau, 2021

2. Arbeitsblatt zum Testen der RSA-Verschlüsselung

Legen Sie Ihr Schlüsselpaar fest und übertragen Sie einen selbst gewählten Buchstaben an Ihren Kommunikationspartner!

Für die Wahl des Schlüsselpaares benötigen Sie Primzahlen.

Damit Sie Ihren zu übertragenden Buchstaben in eine Zahl und die Zahl beim Empfang einer Nachricht wieder in einen Buchstaben umwandeln können, ist hier die Liste der deutschen Großbuchstaben des ASCII-Codes:

65 = A	**66 = B**	**67 = C**	**68 = D**	**69 = E**	**70 = F**	**71 = G**	**72 = H**	**73 = I**
74 = J	**75 = K**	**76 = L**	**77 = M**	**78 = N**	**79 = O**	**80 = P**	**81 = Q**	**82 = R**
83 = S	**84 = T**	**85 = U**	**86 = V**	**87 = W**	**88 = X**	**89 = Y**	**90 = Z**	

Nachricht mit RSA verschlüsseln	Nachricht mit RSA entschlüsseln
E: Vorbereitungen: ***p*** wählen: _____ ***q*** wählen: _____ ***e*** wählen: _____	**E: Verschlüsselte Nachricht *C* und privaten Schlüssel *d* bereit halten:** ***C***: _____ ***d***: _____
E: Privaten Schlüssel aus *p*, *q* und *e* ermitteln: *d* berechnen: _____ (Excel-Tabelle)	**E: N des öffentlichen Schlüssels bereit halten:** ***N***: _____
E: Öffentlichen Schlüssel aus *p*, *q* und *e* ermitteln: ***N*** berechnen: _____ ($N = p \cdot q$) ***e*** notieren: _____ (siehe oben)	**E: *C* entschlüsseln, um *M* zu erhalten:** $M = C^d \bmod N$ ***M*** = _____ (Windows-TR)
E: Öffentlichen Schlüssel (*N*, *e*) an Sender übermitteln	**E: Zahl *M* in ASCII-Zeichen umwandeln:** *ASCII-**Zeichen***: _____ (ASCII-Liste)
S: Zeichen, das übertragen werden soll, bestimmen: ASCII-**Zeichen**: ____ ASCII-**Nummer *M***: ____ (ASCII-Liste)	**E: hat die Nachricht entschlüsselt. Das ASCII-Zeichen ist die ursprüngliche Nachricht des Senders.**
S: Zahl *M* verschlüsseln: $C = M^e \bmod N$ = _____ (Windows-TR)	
S: Verschlüsselte Nachricht *C* an Empfänger E übermitteln	

E steht für die Tätigkeiten, die der **Empfänger** der Nachricht ausführen muss, **S** für die Aufgaben, die der **Sender** der Nachricht abarbeiten muss.