DIE RSA – VERSCHLÜSSELUNG

In der zweiten Hälfte des 20. Jahrhunderts begann man sich mit dem Problem des Schlüsseltausches zu beschäftigen. Als narrensichere Verschlüsselung bewährt sich das One Time Pad, eine Methode, bei der der Schlüssel so lang ist, wie der zu verschlüsselnde Text. Ein One Time Pad ist unmöglich zu entschlüsseln, wenn man es wirklich nur einmal benützt. Im aufkommenden Elektronik-Zeitalter erwiese sich aber die Schlüsselverteilung als ständig wachsendes logistisches Problem (Internet gibt es seit 1982).

Das Trio Whitfield Diffie, Martin Hellmann und Ralph Merkle befasste sich ab 1974 intensiv mit dem Problem. Sie suchten nach Funktionen, die sich nicht umkehren lassen und wurden fündig bei den Modulfunktionen: $a \bmod N$ ist in Excel: $=\text{REST}(a;N)$. Mit Modulfunktionen rechnen Sie problemlos seit Ihrer Mittelstufenzeit: $0547 + 18\text{Min} = 0605$ oder: $930 + 6\,\text{h} = 1530$ (beim ersten Beispiel mod 60, beim zweiten mod 12).

1976 fand Hellmann eine Methode, mit der Alice und Bob öffentlich (Internet, Telefon) Schlüsselzahlen austauschen können, mit denen ein dritter nichts anfangen kann. Betrachten Sie die folgende Tabelle:

x	1	2	3	4	5	6	7	8	9	10
5^x	5	25	125	625	3125	15625	78125	390625	1953125	9765625
$5^x \bmod 7$	5	4	6	2	3	1	5	4	6	2

Für kleine Zahlen wie 5 und 7 kann man durch fleissiges Probieren auf mögliche Lösungen kommen: $5^x \bmod 7 = 2 \quad \Rightarrow \quad x = 4$ aber auch $x = 10$, $x = 16$ u.s.w. Tatsächlich werden aber für die Basis sehr grosse Zahlen benützt.

1975 bewies Diffie die technische Möglichkeit einer asymmetrischen Verschlüsselung: Alic veröffentlicht Einzelheiten zu ihrem Schlüssel, die jedermann benützen kann, den aber nur sie selber entschlüsseln kann. Anschauliches Beispiel dazu: Alice stellt offene Vorhangschlösser zur Verfügung. Bob kann seine Botschaft in eine Kiste legen und das Schloss zuschnappen lassen. Nur Alice hat den Schlüssel, um es wieder zu öffnen.

Auf Grund dieser Entdeckung entwickelte das Team Ron **R**ivest, Adi **S**hamir und Leonard **A**dleman das **RSA** – Verfahren. Ein Jahr lang entwickelten Rivest und Shamir immer wieder neue Ideen, die dann von Adleman zerfleddert wurden. 1977 konnte Rivest nach einem Zechabend nicht einschlaffen und plötzlich zündete der entscheidende Funke. Grundlage ist das Produkt zweier sehr grosser Primzahlen. Versuchen Sie einmal die Zahl 408'508'091 mit dem Taschenrechner in Ihre Faktoren zu zerlegen. Ist dieses Produkt aber in der Grössenordnung 10^{308} würden hundert Millionen PCs mehr als tausend Jahre brauchen, um die Faktorzerlegung zu finden (Zahlen von 1999).

1977 druckte Martin Gardener einen verschlüsselten Text ab und dazu eine Zahl N in der Grössenordnung 10^{129}. 1994 gelang einer Gruppe von 600 Personen die Entschlüsselung!

Das Verfahren wird in der Tabelle auf Seite 4 beschrieben – natürlich mit sehr kleinen Zahlen. Excel kann höchstens 10-stellige Zahlen exakt verarbeiten.

Tabelle "Daten"

RSA.xls

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1														
2														
3		**p**	**11**		p,q von Alice gewählt und geheim gehalten									
4		**q**	**13**											
5		**e**	**11**		von Alice gewählt; teilerfremd zu (p-1)(q-1)									
6		N	**143**		N=pq									
7														
8														
9														
10		d berechnen, sodass: ed=1 mod (p-1)(q-1)					NN=(p-1)(q-1)=	120						
11														
12		**d**	**11**								ed	ed mod NN	d	
13										1	11	11		
14										2	22	22		
15										3	33	33		
16										4	44	44		
17										5	55	55		
18										6	66	66		
19										7	77	77		
20										8	88	88		
21										9	99	99		
22										10	110	110		
23										11	121	1	11	
24										0	0	0		
25										0	0	0		

Daten | Vorgang | a^x mod N

Die Zahlen in C3..C5 werden eingegeben. Alle fetten Zahlen werden benannt.
Diese Namen gelten in allen drei Tabellen!

Um d zu berechnen bilden wir so lange Vielfache von e bis der Modul 1 ergibt.

Der Wert d ist die Summe der Spalte M.

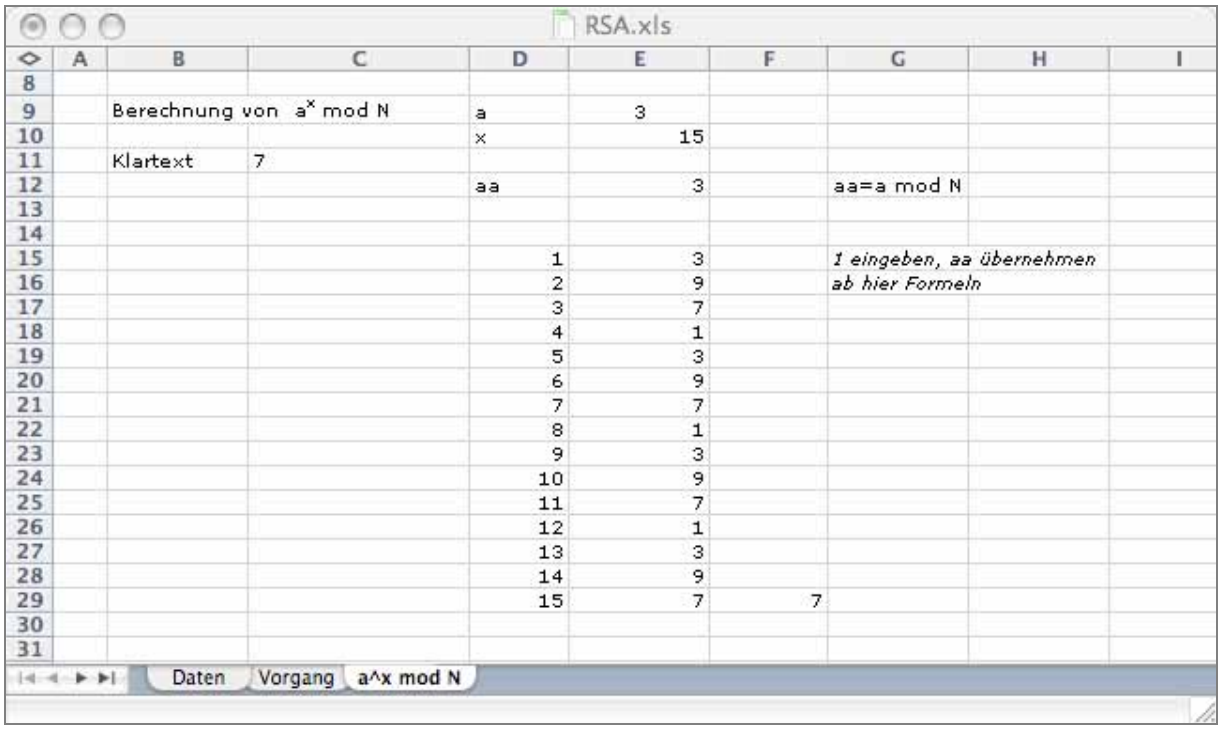
Die Formeln in den Spalten J bis M werden einfacher, wenn man statt leeren Feldern eine Null schreibt. Diese Nullen kann man mit einem kleinen Trick verschwinden lassen:

Spalten J bis M markieren
Format → Bedingte Formatierung

unter Format die Schriftfarbe weiss wählen
Hinzufügen

Tabelle "a^x mod N"

Hier werden die Daten ver- oder entschlüsselt.



	A	B	C	D	E	F	G	H	I
8									
9		Berechnung von a^x mod N		a	3				
10				x	15				
11		Klartext	7						
12				aa	3		aa=a mod N		
13									
14									
15				1	3		*1 eingeben, aa übernehmen*		
16				2	9		*ab hier Formeln*		
17				3	7				
18				4	1				
19				5	3				
20				6	9				
21				7	7				
22				8	1				
23				9	3				
24				10	9				
25				11	7				
26				12	1				
27				13	3				
28				14	9				
29				15	7	7			
30									
31									

a, x, aa sind Namen der danebenliegenden Zellen.

Die Zahlen in E9 und E10 können beliebig gesetzt werden; mit den Makros werden wir Sie aus der vorhergehenden Tabelle holen. N ist in Tabelle 1 definiert.

Excel ist mit Potenzen sehr rasch überfordert (323 ist der letzte Wert, der noch exakt dargestellt wird); deshalb müssen wir in Stufen rechnen:

Für das Beispiel oben im Blatt "Tabelle" p = 5 und q = 2 setzen.

Wir rechnen $3^{15} = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3$ und bilden nach jedem Zwischenresultat den mod aus:

$3 = 3 \bmod 10 = \mathbf{3}$

$\mathbf{3} \cdot 3 \bmod 10 = 9 \bmod 10 = \mathbf{9}$

$\mathbf{9} \cdot 3 \bmod 10 = 27 \bmod 10 = \mathbf{7}$

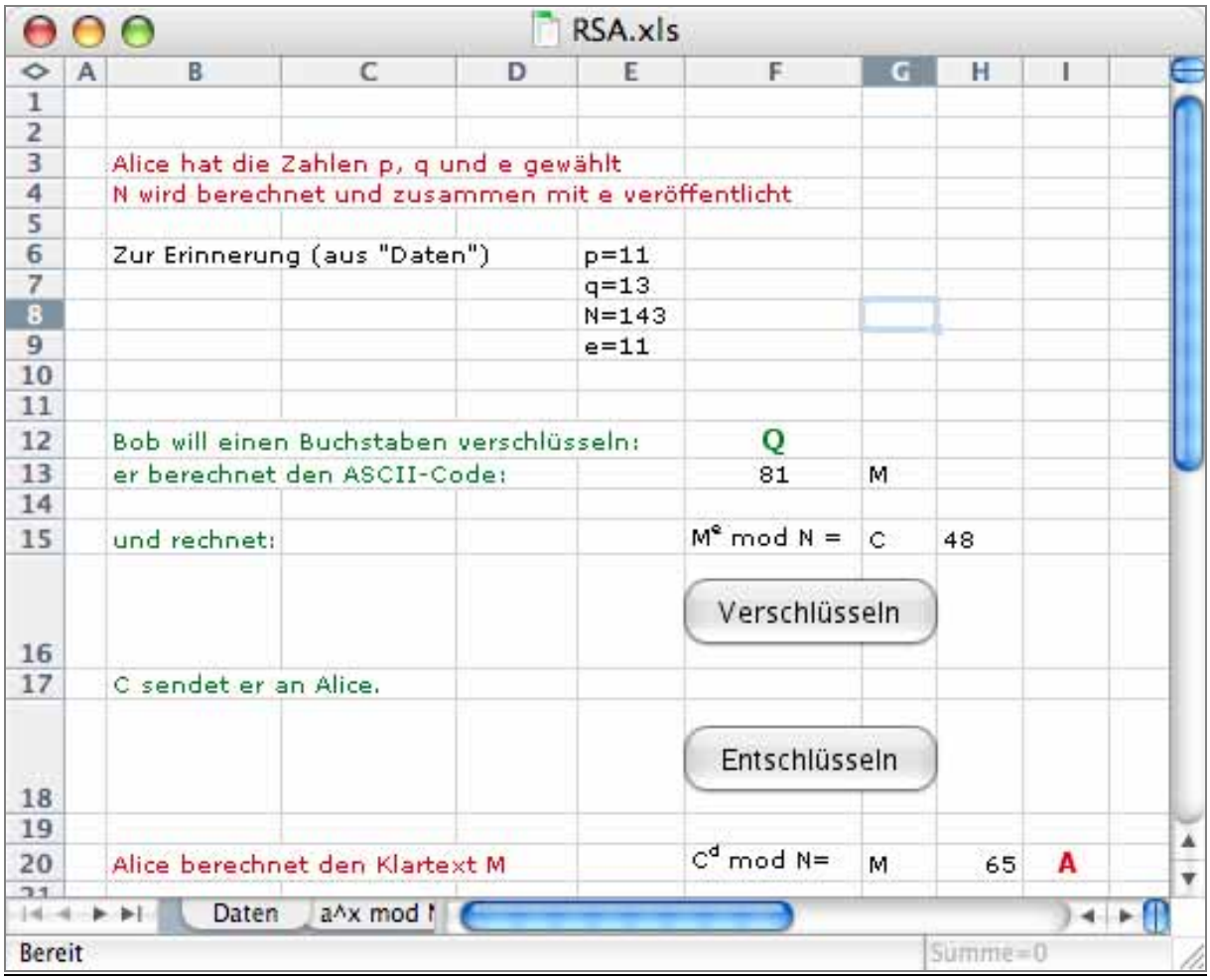
$\mathbf{7} \cdot 3 \bmod 10 = 21 \bmod 10 = \mathbf{1}$

u.s.w.

Die Formelreihen in D, E und F sind länger; die Zahlenreihe wird nur ausgerechnet, bis der Exponent x erreicht ist.

Der Klartext in C11 ist die Summe der Spalte E.

Tabelle "Vorgang"



M und C sind als Namen für die zugehörigen Zellen F13 und H15 zu definieren.

In E6..E9 stehen Textformeln.

Kernstück sind die beiden Makros, die Sie vor dem Aufzeichnenlassen unbedingt ein paar Mal durchspielen sollten:

Verschlüsseln: F13 kopieren
nach Tabelle "a^x mod n wechseln
in E9 als Wert einsetzen (warum?)
in E10 die Formel =e schreiben
C11 kopieren
nach Tabelle "Vorgang" wechseln
in H15 als Wert einsetzen

Überlegen Sie selber, wie das Makro "Entschlüsseln" abläuft.