

Unsere bisherigen Überlegungen haben gezeigt, dass das RSA-Verfahren ein asymmetrisches aber eben leider nur monoalphabetisches Substitutionsverfahren ist, mit dessen Hilfe das Schlüsselübermittlungsproblem gelöst werden könnte.

Bei einer einfachen, zeichenweisen Verschlüsselung wäre dieses Verfahren allerdings schon bei kürzeren Texten völlig ungenügend, da es als monoalphabetisches Substitutionsverfahren leicht über eine statistische Analyse zu „knacken“ wäre.

Dieser Nachteil hat allerdings in der Praxis keine Bedeutung, da dort mit Schlüssellängen von 1024 oder gar 2048 Bit (für den Modulwert) verwendet werden. Dies bedeutet, dass man mit einem Rechengang einen Block von bis zu 128 Byte (Zeichen) oder sogar 256 Byte (Zeichen) verschlüsseln kann. Bis zu 256 Klartextzeichen „verschwinden“ dabei in einem einzigen Geheimtextwert.

Da das Rechnen mit solch langen Dualzahlen auch für einen modernen Rechner sehr aufwändig ist, vermeidet man, mit Rücksicht auf die Verarbeitungsgeschwindigkeit, längere Texte mit einem solchen asymmetrischen Verfahren zu verschlüsseln. Dazu sind moderne symmetrische Verfahren wie AES rundum besser geeignet. Diese Verfahren, bei denen die Klartextzeichen durch eine mehrfache Kombination von blockorientierten Transpositions- und Substitutionsrunden regelrecht verwirbelt werden, arbeiten mit maximalen Schlüssellängen von 256 Bit. Dies bedeutet, dass der ganze Schlüssel für ein solch schnelles und zuverlässiges symmetrischen Verfahren problemlos in einem einzigen RSA-Wert verschlüsselt werden kann.

Der Effekt einer Blockchiffrierung soll wegen der beschränkten Kapazität unseres „Taschenrechners“ an folgendem vereinfachten Beispiel demonstriert werden. Damit wir noch innerhalb der mit unserem „Taschenrechner“ berechenbaren Werte bleiben, ist das Beispiel so gewählt, dass jeweils ein Buchstabe ausnahmsweise nicht mit 8 Bit, sondern mit 4 Bit dargestellt werden kann. So können wir wenigstens immer 3 Zeichen zu einem Block zusammenfassen und gemeinsam verschlüsseln, ohne einen „overflow“ zu provozieren.

Gegeben sei deshalb folgende Tabelle, in welcher den Buchstaben A – N folgende Werte zugeordnet sind:

Klartextzeichen	A	B	C	D	E	F	G	H	I	J	K	L	M	N
dezimal	2	3	4	5	6	7	8	9	10	11	12	13	14	15
binär	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

Eine **zeichenweise Chiffrierung** des Vornamens „ELE“ würde zu folgendem Geheimtext führen: *(Schon eine einfache Geheimtextanalyse zeigt, dass hier zweimal das selbe Zeichen verschlüsselt wurde.)*

Klartext:            E            L            E  
 Dezimalwert:    (6)        (13)      (6)  
 Geheimtext:    **3.878    1.405    3878**

public key	private key
53, 4223	77, 4223

Bei einer **Blockchiffrierung** wird wie folgt vorgegangen:

Klartext:	E	L	E
Binärwert:	0110	1101	0110
Ergibt zu einem 12-Bitwert zusammengezogen (Bitblock):	011011010110		
Diesem 12-Bit-Dualwert entspricht der Dezimalwert:	1.750		
Bei der Verschlüsselung ergibt $1.750^{53} \text{ mod } 4223$ als Geheimtextwert:	<b>2.162</b>		

*Beim Chiffrieren werden mehrere Zeichen zu einer langen Bitkette (Block) zusammengefasst. Dieser Bitkette wird insgesamt als ein Zahlenwert betrachtet und als solcher verschlüsselt.*

Ergibt dechiffriert: $2.162^{77} \text{ mod } 4223 =$	1.750		
Diesem Dezimalwert entspricht der 12-Bit-Dualwert	011011010110		
aufgeteilt in 4-er-Gruppen	0110	1101	0110
ergibt sich der dechiffrierte Klartext:	E	L	E

*Beim Dechiffrieren wird der Geheimtext zunächst als Block dechiffriert. Danach wird der Ergebnis-Bitblock wieder in die einzelne Zeichen aufgeteilt. (Die bei uns ausnahmsweise mal nur 4 Bit lang waren.)*