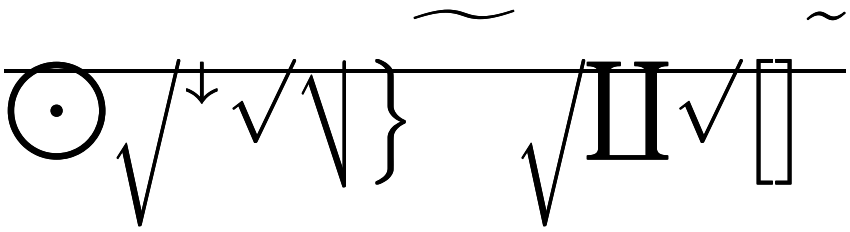

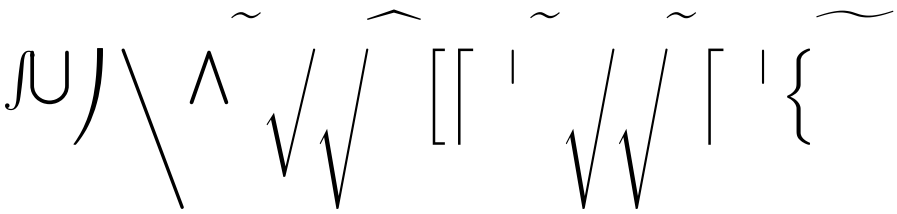

Generelles:
M: Nachricht (Message)
N: Öffentliches Schloss
e: (Halb-)Öffentlicher Schlüssel → zum Codieren (encrypt)
d: Privater Schlüssel → zum Decodieren (decrypt)
C: Verschlüsselte Nachricht (Cypher)

p&q: Sehr große Primzahlen zur Schlüsselberechnung
N = p*q
e = Eine selbst ausgewählte Primzahl; Vorraussetzungen: [1<e<N, e ist ungleich p und q]
d = Eine weitere Primzahl mit den Vorraussetzungen: [e*d mod((p-1)(q-1))=1; 1<d<N]

Encrypt: C = M^e mod(N)
Decrypt: M = C^d mod(N)

Bestimmung von d:

	e*d mod((p-1)(q-1)) = 1
Generell:	a mod(b) = 1
Also:	a:b = x mit Rest 1 → a ist 1 zu groß um ein Vielfaches von b zu sein
Daher:	(a-1):b = x ohne Rest ➔ (a-1) ist ein Vielfaches von b
Daraus ergibt sich:	k*b = a-1
Zurückgeformt:	e*d mod((p-1)(q-1)) = 1
	→k*(p-1)(q-1) = e*d -1 | +1 | /e
	➔d = (k*(p-1)(q-1)+1)/e

p, q, und e sind bekannt, daher muss die Vielfache k bestimmt werden.
Man nutzt hierzu die Sequence-Funktion des TI84. Man erstellt eine Liste z.B. von 1 bis 200 und setzt im Header einer zweiten Liste die erste Liste für k in die oben genannte Formel für d ein. Hier kommen nun in diesem Beispiel 200 Werte für d heraus. Da, wie bereits genannt, d einige Voraussetzungen erfüllen muss, können wir in der zweiten Liste sehr bequem einen Wert für d finden. Dieser Wert muss kleiner sein als N, größer als 1, eine ganze Zahl und eine Primzahl. Man durchsucht also die Liste nach einem Wert auf den die Voraussetzungen zutreffen und benennt diesen als d.

Mit dieser Methode lassen sich privater und öffentlicher Schlüssel sehr einfach bestimmen und schon kann man Nachrichten verschlüsseln.

PS: Die Sequence-Funktion:
Im Tabellenkopf wird eingetippt:
2nd→ Catalog → S → seq(➔ seq(X, X, 1, 200)