Mit RSA Daten verschlüsselt austauschen

Aufgaben:

1. **Wähle** ein Schlüsselsystem aus, bei dem n > 32.000.000 ist.
   Die RSA-Demo von *CrypTool* und folgende Information werden dir dabei behilflich sein:
   $2^{24} = 16.777.216$ $2^{25} = 33.554.432$ $2^{26} = 67.108.864$
2. **Tausche** mit einem Partner die öffentlichen Schlüssel aus!
3. **Fasse** dein Geburtsdatum in einer großen Zahl **zusammen**, die aus den Ziffern deines Geburtsdatums in der Reihenfolge **ttmmjjjj** besteht!
   Beispiel: 23.5.1991 → 23051991 (Die Null nicht vergessen, falls Tag oder Monat < 10!)
4. **Verschlüssle** dein Geburtsdatum mit dem **öffentlichen** Schlüssel **deines Partners**!
   Nutze dazu die RSA-Demo von *CrypTool*!
5. **Tauscht** nun die **verschlüsselten** Geburtstage per E-Mail aus!
6. **Entschlüssle** das Geburtsdatum deines Partners mit **deinem geheimen** Schlüssel!
   Nutze dazu die RSA-Demo von *CrypTool*!

Mein Schlüsselsystem	**Schlüsselsystem deines Partners**
mein **geheimer Schlüssel:**	sein **geheimer Schlüssel:**
	
mein **öffentlicher Schlüssel:**	sein **öffentlicher Schlüssel:**
	

Verschlüsselung meines eigenen Geburtsdatums:

Entschlüsselung des Geburtsdatums meines Partners: