

3. Geheimnisse weltweit

Q: Übrigens Bond. Mit dem Verfahren können sie natürlich auch mit 006 und 008 direkt Kontakt aufnehmen.

Also los, versetzt euch in die Rolle der Geheimagenten ihrer Majestät. Baut eure eigene Public-Key-Infrastruktur (PKI) auf: Schickt euch gegenseitig eure öffentlichen Schlüssel und sendet euch geheime Nachrichten.

Tip: Im Handschuhfach des Z8 hat Moneypenny die öffentlichen Schlüssel abgelegt, die sie von euch und euren Kollegen bekommen hat.

(Auch hier könnt ihr die in MuPAD für das Versenden und Empfangen per Email von Q eingebauten Funktionen `mailto`, `checkmail`, `readmail` verwenden. Um von der obigen WWW-Seite den öffentlichen Schlüssel des gewünschten Empfängers in eure MuPAD Sitzung zu bekommen, folgt einfach den Anweisung dort. Jetzt müßt ihr eure Nachricht mit dem öffentlichen Schlüssel von `sk06-z8-77` verschlüsseln und dann etwa so verschicken:

```
mailto( "sk06-z8-77@bit.uni-bonn.de", "von uns an Z8-77", N, e, y );
```

Mail empfangen geht genau wie vorher bei Moneypenny ... Aber achtet darauf, dass ihr Euren eigenen Schlüssel verwendet.)

Q: Bond, ich brauche sie ja wohl nicht darauf aufmerksam zu machen, warum RSA funktioniert?

Fragen und Anregungen

- *Wisst ihr, warum RSA funktioniert?*
- *Versucht doch mal, für welche k die Gleichheit $x^k \bmod p = 1$ gilt, wenn ihr für p eine kleine Primzahl nehmt, etwa $p = 7$ oder $p = 13$. Tipp: MuPAD kann auch Schleifen, z.B.:*

```
for k from 1 to 5 do
  print(k);
end_for;
```

Wie hängt eure Antwort von p ab?