

2. Baku, am Hafen neben Bond's Z8

Julietta: Mister Bond?

Bond: Ja?

Julietta: Moneypenny schickt mich, sie hat eine wichtige Nachricht. Sie sollen sich sofort per Email bei ihr melden,

moneypenny@mi6.gov.uk,

es geht um Leben und Tod.

Bond: Ja, die gute, alte Moneypenny. Dann will ich mir mal ein paar nette Primzahlen einfallen lassen.

Und ... Julietta? Haben sie danach schon etwas vor?

Helpf Bond und schickt Moneypenny eine Email mit eurem öffentlichen Schlüssel.

(Q hat in MuPAD für das Versenden und Empfangen per Email die Funktionen mailto, checkmail, readmail eingebaut. Die formatieren die Mail auch automatisch richtig, was nicht unbedingt so einfach ist, wie es aussieht. Beispiel:

```
mailto( "moneypenny@mi6.gov.uk", "Hier Oskar", N, e );
```

... und jetzt auf die Antwort warten ...

```
checkmail();  
readmail( 1 );
```

Jetzt müsst ihr nur noch entschlüsseln. . .

Ach, solltet Ihr inzwischen Euren geheimen Schlüssel (N, d) überschrieben haben, dann könnt Ihr ihn mit `retrievesecretkey(N, e)` zurückholen. Nach `readmail()` hilft `retrievesecretkey(msgN, msge)`, wenn man seinen Schlüssel verlegt hat.)

Julietta: Q sagte mir noch, sie sollen auf gar keinen Fall $x^e \bmod N$ statt `powermod(x, e, N)` schreiben.

Fragen und Anregungen

- *Klar, dass Bond nicht auf Q hört. Was passiert, wenn ihr Qs Rat in den Wind schlagt?*
- *Besucht das Additionskettenspiel.*