

1. London, im Keller des Secret Service

Q: Natürlich weiß ich, dass sie die besten Verschlüsselungstechniken der Welt kennen. Aber seit ihrem letzten Einsatz waren wir nicht untätig. Unsere Spezialisten haben das RSA-Verfahren von Rivest, Shamir & Adleman so einfach gemacht, dass Moneypenny ihnen wichtige Informationen sogar durch unzuverlässige Boten schicken kann.

Bond: Ich erinnere mich an Shamir. Er ist Israeli und arbeitet am Weizmann Institut, richtig?

Q: Ja. Hier ist eine Demonstration des Verfahrens, sie sollten keine Schwierigkeiten haben, es auf dem Laptop in der Konsole ihres neuen BMW Z8 zu implementieren.

Hoppla, jetzt sind mir die Karten heruntergefallen und vollkommen durcheinandergeraten. Naja, kein Problem für sie, Bond.

Nehmt Bond die Arbeit ab! (Startet MuPAD, indem ihr den auf den Startknopf Eures Z8 drückt.)

Q: Bond! Bitte bringen sie den Wagen diesmal heile zurück.

Bond (nach kurzer Durchsicht der Karten): Q, ihnen ist doch klar, dass das so, wie es hier steht, jeder knacken kann?

Q: Natürlich müssen sie größere Zahlen nehmen. Aber außerdem müssen sie darauf achten, immer lange Textstücke zu einer Zahl zusammenzufassen.

Fragen

- *Warum ist es Q so wichtig, möglichst lange Textstücke direkt durch RSA zu schleusen?*
- *Wäre es nicht genug, einzelne Buchstaben mit riesigen Primzahlen zu verschlüsseln, wenn man mal davon absieht, dass eine Nachricht dadurch ungeheuer aufgeblasen wird?*
- *Was muss beachtet werden, damit das System sicher ist?*

Mit euren Antworten erreicht ihr den nächsten Einsatzort.