2.5. Beirut, Libanon

004: Hallo Moneypenny!

Moneypenny: Hallo Frederick!

004: Ich habe von euch gestern eine Nachricht erhalten, mit welchem Zahlencode man Kamal Kahns Bombe entschärfen kann. Ich fürchte allerdings, dass die Nachricht unterwegs von Kahns Männern abgefangen wurde und durch einen anderen Zahlencode ersetzt wurde. Bitte schicken Sie mir den Code nochmals und unterschreiben Sie die Nachricht elektronisch.

Moneypenny: Mit welchem Verfahren?

004: Benutzen Sie doch das RSA-Signatur Verfahren.

Moneypenny: Wie funktioniert das nochmal?

004: Ganz einfach: Wenn Sie den Code signieren, verschlüsseln Sie ihn einfach mit Ihrem geheimen Schlüssel.

Überlegt euch, dass dies tatsächlich funktioniert. Nehmt dazu eine beliebige Zahl und verschlüsselt Sie mit eurem geheimen *Schlüssel. Wie würdet ihr die Signatur alleine mit dem öffentlichen Schlüssel überprüfen?*

Moneypenny: Ich habe nun die Nachricht verschickt.

004: Sehr schön, dann entschärfe ich nun die Bombe.

Fragen

- *Nach Erhalt der Nachricht verifiziert 004 Moneypennys Signatur und versucht den Code in die Bombe einzugeben. Diese explodiert und er stirbt. Was könnte unterwegs mit der Nachricht geschehen sein? Hinweis: Kamal Kahn konnte einfach eine Signatur zufällig auswählen und diese mit Moneypennys öffentlichen Schlüssel verschlüsseln. Dann...*
- *Überlegt euch, wie man einen solchen Angriff abwehren könnte. Hinweis: Nehmt an, ihr habt eine Funktion, die beliebige Nachrichten in Zahlen verwandeln kann (also gewissermaßen einen Fingerabdruck der Nachricht erzeugt) und die man nicht leicht invertieren kann (mit anderen Worten eine Einwegfunktion).*