Codierungs-, Kompressions-, und
Verschlüsselungsverfahren einsetzen

Aufgabe 1 (RSA Verfahren)

Als Einstieg werden Sie einfache Modulo Berechnungen durchführen:

89 (mod 10) ≡	45 (mod 8) + 19 (mod 8) ≡
54 (mod 5) ≡	45 (mod 8) · 19 (mod 8) ≡
22 (mod 16) ≡	(4 · 13) (mod 9) ≡

Welche Zahlenkombinationen sind teilerfremd? Geben Sie für die anderen mind. einen Teiler an.

46	53		17	102	
67	45		100	201	
45	93		60	1239	

Nun generieren Sie selber ein RSA Schlüsselpaar mit den Anfangswerten:

1.) p = 7 q = 11 e = 13 2.) p = 13 q = 17 e = 5

Berechnung öffentlicher Schlüssel:

Privater Schlüssel: Übernehmen Sie die Rolle von Bob und verschlüssen Sie mit Paar 1.) seinen Namen. Setzen Sie B auf 2 und O auf 15. Verwenden Sie zum Berechnen der Werte den Windows TR.

Im Klassenordner finden Sie das Excelprogramm 05_3RSA.xlxs. Generieren Sie mit dessen Hilfe zu den Primzahlpaaren 1.) und 2.) je drei weitere Schlüsselpaare.

Vervollständigen Sie die Exel-Arbeitsmappe, indem Sie für die Ver- und Entschlüsselungs-Tabs Formeln einsetzen.

= code("TEXT") Zeichen --> ASCII-Code, = zeichen(WERT) ASCII-Code --> Zeichen
= rest (ZAHL;DIVISOR) --> Restberechnung, = potenz (BASIS,EXPONENT) --> Potenz