Arbeitsblatt zum Testen der RSA-Verschlüsselung

Jetzt dürfen Sie! Legen Sie Ihr Schlüsselpaar fest und übertragen Sie einen selbst gewählten Buchstaben an Ihren Kommunikationspartner!

Für die Wahl des Schlüsselpaares benötigen Sie Primzahlen. Damit die Berechnungen mit dem Windows-Taschenrechner noch möglich sind, verwenden wir nur Primzahlen kleiner als 100. Hier sind alle Primzahlen von 1 – 100:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Damit Sie Ihren zu übertragenden Buchstaben in eine Zahl und die Zahl beim Empfang einer Nachricht wieder in einen Buchstaben umwandeln können, ist hier die Liste der deutschen Großbuchstaben des ASCII-Code:

65 = A	**66 = B**	**67 = C**	**68 = D**	**69 = E**	**70 = F**	**71 = G**	**72 = H**	**73 = I**
74 = J	**75 = K**	**76 =L**	**77 = M**	**78 = N**	**79 = O**	**80 = P**	**81 = Q**	**82 = R**
83 = S	**84 = T**	**85 = U**	**86 = V**	**87 = W**	**88 = X**	**89 = Y**	**90 = Z**	

Nachricht mit RSA verschlüsseln	Nachricht mit RSA entschlüsseln
E: Vorbereitungen: *p* wählen: 67 (Primzahl-Liste) *q* wählen: 59 (Primzahl-Liste) *e* wählen: 7 (Primzahl-Liste)	**E: Verschlüsselte Nachricht *C* und privaten Schlüssel *d* bereit halten:** *C*: 224 *d*: 547
E: Privaten Schlüssel aus *p*, *q* und *e* ermitteln: *d* berechnen: 547	**E: Teil *N* des öffentlichen Schlüssels bereit halten** *N*: 3953
E: Öffentlichen Schlüssel aus *p*, *q* und *e* ermitteln: *N* berechnen: 3953 ($N = p \cdot q$) *e* notieren: 7 (siehe oben)	**E: *C* entschlüsseln, um *M* zu erhalten:** $M = C^d \bmod N$ *M* = 83 (Windows-Taschenrechner)
E: Öffentlichen Schlüssel (*N*, *e*) an Sender übermitteln	**E: Zahl *M* in ASCII-Zeichen umwandeln:** *ASCII-Zeichen*: S (ASCII-Liste)
S: Zeichen, das übertragen werden soll, bestimmen: ASCII-**Zeichen**: S ASCII-**Nummer** *M*: 83 (ASCII-Liste)	**E: hat die Nachricht entschlüsselt. Das ASCII-Zeichen ist die ursprüngliche Nachricht des Senders.**
S: Zahl *M* verschlüsseln: $C = M^e \bmod N = 224$ (Win-Rechner)	
S: Verschlüsselte Nachricht *C* an Empfänger E übermitteln	

E steht für die Tätigkeiten, die der **Empfänger** der Nachricht ausführen muss, **S** für die Aufgaben, die der **Sender** der Nachricht abarbeiten muss.