



Code Knacken



Die NSA will eine unbekannte Zahl $a = a_7$ decodieren, also entschlüsseln oder bestimmen, die von Internetfirmen zur Verschlüsselung von Kundendaten benutzt wird. Die NSA kennt aber nur die verschlüsselte siebenstellige Zahl $y = 8504798$ und weiß einiges über den Codierungsprozess:

Aus der gesuchten Zahl a_7 berechnet sich die gegebene, öffentliche Zahl y folgendermaßen:

Wir definieren die Ziffern x_i von a_7 mittels $a = a_7 = x_7x_6x_5x_4x_3x_2x_1$

Streicht man die letzte Stelle x_1 , ergibt sich eine Zahl $a_6 = x_7x_6x_5x_4x_3x_2$

Streicht man in a_6 wieder die letzte Stelle, ergibt sich a_5 , usw. bis zu $a_1 = x_7$.

Die bekannte Zahl y ergibt sich aus der gesuchten Zahl a_7 durch die Formel:

$$y = a_7 + a_6 + a_5 + a_4 + a_3 + a_2 + a_1.$$

Man bestimme aus dieser Information x_1 bis x_7 und damit a .

Beispiel Verschlüsselung:

Originalzahl $a = 1111111$ ergibt verschlüsselte Zahl

$$y = 1111111 + 1111111 + 1111111 + 111111 + 111111 + 11111 + 1111 + 111 + 11 + 1 = 1234567$$

Für Hartgesottene: Löse dasselbe Problem für 15-stellige Zahlen und $y = 603567764060350$.