Chiffrendesign

Will man ein Verschlüsselungsverfahren entwickeln, bieten sich zwei Wege an:

- Man macht das Verfahren möglichst kompliziert und hofft, dass dadurch keine Schwachstellen entstehen – oder dass ein Angreifer diese in der Komplexität nicht findet. Diesen Ansatz nennt man auch "Security by Intricacy" (in etwa "Sicherheit durch Unduchschaubarkeit")
- Man entwirft das Verfahren möglichst durchdacht und versucht, Schwachstellen gar nicht entstehen zu lassen.

Wenig verwunderlich kommt bei ernsthaften Verfahren nur die zweite Variante zum Einsatz.

Was ist eine Schwachstelle eines modernen Verfahrens?

Zunächst muss man sich klarmachen, was man bei modernen Verfahren unter einer Schwachstelle versteht.

Bei einem modernen Verfahren spricht man bereits dann von einer "Schwachstelle", wenn es einen Angriff auf das Verfahren gibt, der besser ist als die vollständige Schlüsselsuche.