Verschlüsselungsprogramm o.ä. zum Austausch von Notendateien

Beitrag von „Seph“ vom 2. Februar 2021 10:14

> Zitat von helmut64
>
> Stimmt nicht. Google mal nach "one time pad".
>
> Auch eine astronomische Anzahl möglicher Schlüssel ist keine Sicherheitsgarantie. Bestes Beispiel dafür ist die ENIGMA.

Das OTP ist leider auch nur dann sicher, wenn alle Nebenbedingungen peinlich genau eingehalten werden, was in der Praxis ziemlich unhandlich ist, insbesondere zur Verschlüsselung größerer Datenmengen. Aber stimmt schon, damit hat man theoretisch ein unbrechbares Verfahren an der Hand.

Die Enigma hatte so deutliche kryptografische Schwächen, dass mir noch immer unklar ist, wie das bei der Konstruktion nicht auffallen konnte. Alleine die Umkehrwalzen führen zu einer Schwächung um etwa 13 Größenordnungen. Blöd war auch, dem Konzept "Security through obscurity" zu folgen. Den Fehler macht Deutschland teils immer noch. Ich selbst bin Fan des Kerkhoff´schen Prinzips, Standards wie AES sind diesbezüglich gut implementiert und vor allem durch aufwendige Audit-Verfahren auf Sicherheitslücken geprüft.

Übrigens hat man auch bei einfacher monoalphabetischer Substitution eine extreme Anzahl möglicher Schlüssel, gleichzeitig ist das Verfahren sehr leicht angreifbar.