

Verschlüsselungsprogramm o.ä. zum Austausch von Notendateien

Beitrag von „s3g4“ vom 26. Januar 2021 17:00

Zitat von Philio

7-Zip kann mit AES-256 verschlüsseln, das ist der derzeitige Industriestandard. Aber grundsätzlich kann jede Verschlüsselung geknackt werden, das ist nur eine Frage des Aufwands. Aber ohne deine dienstliche Verordnung zu kennen, vermute ich, dass du nur dafür sorgen musst, dass die Verschlüsselung „hinreichend sicher“ ist. Dass die Verschlüsselung durch Profi-Hacker oder die NSA nicht knackbar ist, erwartet keiner.

Zitat von scrambox

On average, to brute-force attack AES-256, one would need to try 2^{255} keys. (This is the total size of the key space divided by 2, because on average, you'll find the answer after searching half the key space.)

So the time taken to perform this attack, measured in years, is simply $2^{255} / 2,117.8$ trillion.

Expressed as an exponent of 10, that's $2.73 * 10^{61}$. Written in full format:

27,337,893,038,406,611,194,430,009,974,922,940,323,611,067,429,756,962,487,493,203 years.

Die Zeit ist niemandem eine Notenliste wert. 😄