Entropie - Kryptologie

Kunstwort altgriechisch ἐντροπία *entropía*, von ἐν *en* ‚an‘, ‚in‘ und τροπή *tropḗ* ‚Wendung‘, ‚Umkehr‘

Anzahl Bits die mindestens gebraucht werden, um die Information einer Nachrichtenquelle darzustellen. (Intuition, noch keine Definition!)

stets positiv oder null

ein Maß für den Zufall

Stärke eines Passworts

Mindest-Anzahl Bits zur Speicherung

Maß für die „Unordnung“ in Texten

Abgekürzt: H (Eta)

Beispiel 1

- ein Passwort aus 8 Zeichen
- aus dem Satz der folgenden 64 Zeichen
  - ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
- jedes Zeichen im Passwort würde dann 6 Bits Entropie haben
  - denn es gibt 64 = 2^6 mögliche Zeichen
- 6 × 8 = 48 Bits an Entropie
  - entspricht 48 Münzwürfe

Beispiel 2

- zufällige Wörter aus einem Vorrat von 2^{11}= 2,048 Wörtern
- Vier Wörter währen dann 4 × 11 = 44 Bit Entropie
- Fünf Wörter aber schon 55 Bit Entropie, also besser als Beispiel 1

Beispiel 3

- Passwort von 40 Zeichen länge
  - wie beim **RIPEMD-160** hash
- nur Hex Zeichen also 0-9 und A-F = 16 Zeichen = 2^4 Zeichen
- jedes Zeichen im Passwort würde dann 4 Bit an Entropie haben, und 40 Zeichen mal 4 Bit = 160 Bit Entropie

www.wenzlaff.info