
logo.png

IT-Security Cryptography and Secure Communications

Exercise: **Stream Ciphers and RNGs**
Lecturer: *Prof. Dr. Michael Eichberg*
Version: 2024-02-03

1. Test for randomness: Let's assume that we have a sequence of bits generated by some RNG. What is the expected result of using common compression tools (e.g., 7zip, gzip, rar, ...) always using the respective best compression mode?

Solution

No relevant compression should be possible! If so, the randomness is highly questionable. High randomness implies a high entropy and therefore nothing to compress. Effectively the file should even be larger due to the required metadata.