DHBW
Duale Hochschule
Baden-Württemberg
CAS
Center for Advanced Studies

# IT-Security Cryptography and Secure Communications

**Excercise:** **Stream Ciphers and RNGs**
**Lecturer:** *Prof. Dr. Michael Eichberg*
**Version:** 2023-10-14

1. Test for randomnness: 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 compresssion mode?

2. Implement an LCG to study how it behaves when the values of $a$, $c$ (and $m$) change.
   Try to find values that produce a supposedly random sequence.

   Test the RNG with the following value:

```
lcg(seed,a,c,m,number_of_random_values_to_generate)
lcg(1234,8,8,256,100)
lcg(1234,-8,8,256,100)
lcg(1234,-8,8,256,100)
```