Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Information Technology
FH Zentralschweiz

Cryptographic Utilities Exercise

Prof. Dr. Josef F. Bürgler

I.BA_MOVK_MM, Semesterweek 04

If possible, write the solution as a Jupyter notebook. This should run when requested in front of the class.
Due-time: The teacher will check the Jupyter notebooks one week after we discussed the topic!

Exercise 1: MD5, SHA1, SHA256, SHA512

Generate the previsously mentioned hash values of the string `Hello World!`. Do You get the same result as Your neighbour? Check the size of each hash value! What are the corresponding block sizes? Make a table! How many hash values would You have to generate in order to find a collision with a probability of at least 50% (90%)?

Exercise 2: True random number generator

Check if Your computer can generate true random numbers, possibly through some special device? Find out the underlying physical principle (thermal noise, etc.). How can You use the random number generator in the power shell (Windows) or some shell (bash, sh, etc.) on Linux or MAC OS X?
How are true random numbers generated on smart cards? Do some research on the internet!

Exercise 3: Linear congruential random number generator

Compute the period of a **linear congruential number generator** if $m = 11$, $b = 5$, $a = 3$ and $x_0 = 7$ is used. Write down the sequence of random number! What is the maximal size of the period? Adapt the paramters, such that the period is maximal!

Aufgabe 4: LFSR

Construct an LFSR of length 5 which produces the sequence of bits $(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, \ldots)$. What is the period of this LFSR? What is the maximal period? Try to improve this LFSR such that it has maximum period!

Solution: Connection (or feedback) polynomial $C(D) = 1 + D + D^3 + D^5$; recursive formula

$$s_j = \sum_{k=1}^{5} c_k s_{j-k} \bmod 2, = s_{j-1} + s_{j-3} + s_{j-5} \bmod 2, \quad j \geq 5.$$

Period is 15 which can be improved to 31 by adding $c_2 = 1$ as an example! To make computations easy, use the following python code

```python
def lfsr5(seed, taps):
    sr, xor = seed, 0
    while 1:
        for t in taps:
            xor += int(sr[t−1])
        xor %= 2
        sr, xor = str(xor) + sr[:−1], 0
        yield sr
        if sr == seed:
            break

a = lfsr5(’10110’, (5,3,2,1))
[next(a) for j in range(31)]
```

Exercise 4: Is random really random (optional)

Read section 5.4.4 in the *Handbook of Applied Cryptography* by A. Menezes, P. van Oorschot and S. Vanstone [?] (p 181, 182, 183). Here we will only look at the monobit and the two-bit test of example 5.31 in the same book.
Consider the (probably non-random) sequence s of length $n = 160$ obtained by replicating the following sequence four times

$$11100\ 01100\ 01000\ 10100\ 11101\ 11100\ 10010\ 01001$$

Apply the monobit and two-bit test. Based on these two tests, would You say, the sequence random?

Solution: monobit test passed because: $X_1 = 0.4 < 3.8415$; two-bit test passed because: $X_2 = 0.6252 < 3.8415$; sequence would also pass poker test, but not runs and autocorrelation test.

Exercise 5: Probability for a collision

There are 40 people in a room. You bet, that there are at least 2 people with the same birthday. What is the probability, that You win? Use the exact formula as well as the approximation!

Solution: Probility of having two people with the same birthday is 0.882 or 88.2%. Use symbolic python for the exact answer:

```python
from sympy import *
i = symbols(’i’,integer=True)
p = 1 − product((365−i)/365,(i,1,39))
p.evalf()
```

Exercise 6: Probability of a collision

Suppose You use a hash function of length 128 bits. How many hash values would You have to compute in order to find a collision with probability at least 90%? Use the approximate forumula from Slide 14/58:

$$n \approx 2^{(m+1)/2}\sqrt{\ln\left(\frac{1}{1-p}\right)}$$

where $m = 128$ and $p = 0.9$. How much storage would You need, if You need 16 bytes for each hash?

Solution: $n \approx 3.9586\ 10^{19}$; $633'380'000$ terabytes storage.

Have fun with crypto!