JKU Institut für Pervasive Computing

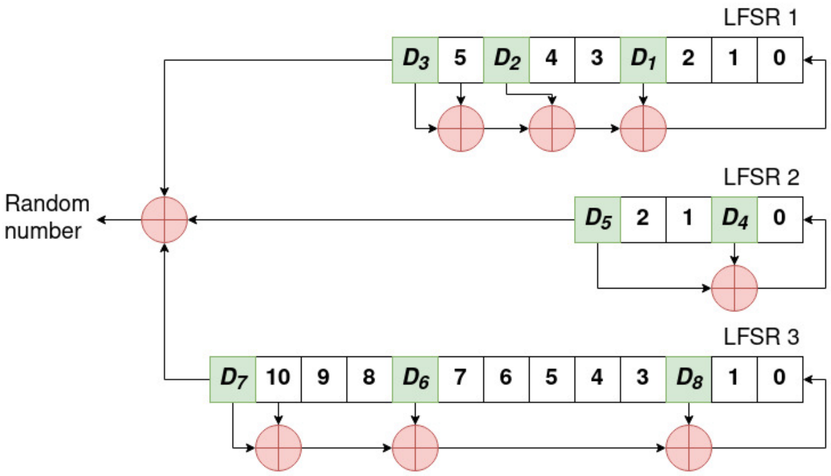
Algorithms and Data Structures 2
Winter term 2021

Assignment 01

Deadline: **Wed 3.11.2021, 23:59**
Submission via: **Moodle**

2. Linear Feedback Shift Register 12 points

Linear Feedback Shift Registers (LFSR) are often used in cryptography. The *A5 algorithm* for instance was used as an encryption algorithm for the first GSM standards for mobile phones. For this exercise we use a slight variation of that algorithm based on three LFSRs.
In fig. 1 the structure of the random number generator is illustrated, after the registers have been initialized, except the placeholders *$D_1..D_8$*. These have to be filled with digits of your personal student ID (according to fig. 2).



LFSR 1
D_3 5 D_2 4 3 D_1 2 1 0
Random number
LFSR 2
D_5 2 1 D_4 0
LFSR 3
D_7 10 9 8 D_6 7 6 5 4 3 D_8 1 0

Fig. 1: Structure of the LFSR random number generator with register contents after initialization.

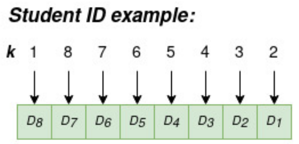


Fig. 2: Mapping of a student ID to placeholders $D_1..D_8$

Algorithm procedure:

1. Link the **leftmost value of each register** with **XOR** ⊕ (eXclusive OR) to calculate the new random number.
2. Calculate the new register values to be inserted on the right end, by linking the appropriate elements again with **XOR**.
3. Finally, shift register contents of all LFSRs to the left and insert the calculated register values from step 2.

For this exercise you have to execute the generator using **pen & paper**. To do so you will find the empty LFSRs on the next page, where you have to **fill in** the **register values** and the **generated random number**. Do this for the first 5 iterations!

Submission:
A PDF containing the first 5 iterations of your personal random number generator. You can print the LFSR skeleton on the next page and scan your final solution, or you can also fill in the skeleton digitally.

JKU Institut für Pervasive Computing

Algorithms and Data Structures 2
Winter term 2021

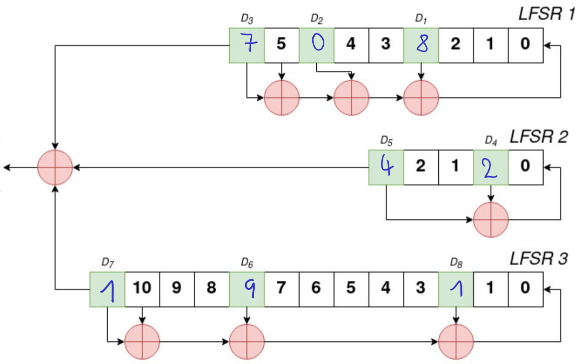
Assignment 01

Deadline: **Wed 3.11.2021, 23:59**
Submission via: **Moodle**

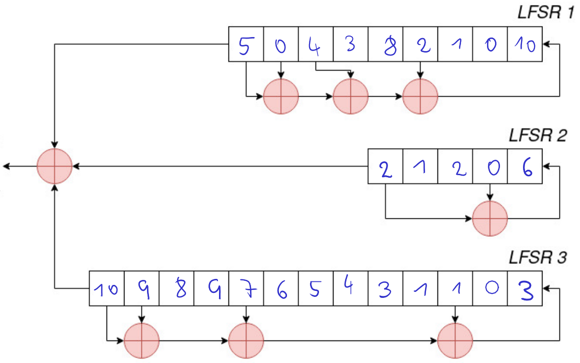
Your student ID:

k	1	1	9	4	2	7	0	8
	D_8	D_7	D_6	D_5	D_4	D_3	D_2	D_1

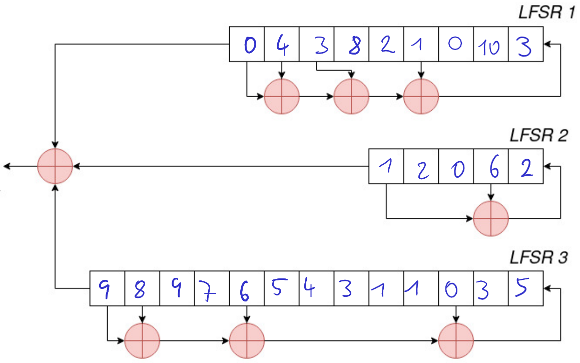
Random number 1: 2



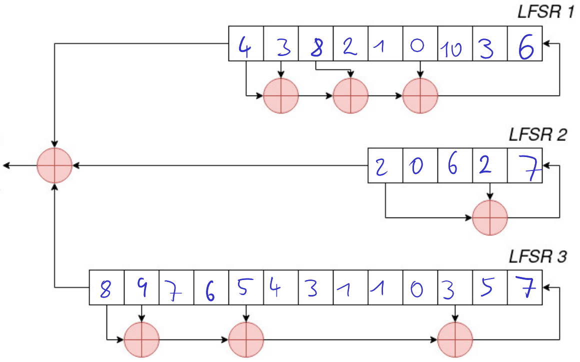
Random number 2: 13



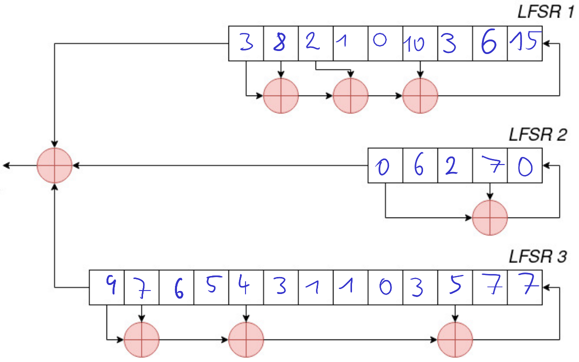
Random number 3: 8



Random number 4: 14



Random number 5: 10


LFSR 1
3 | 8 | 2 | 1 | 0 | 10 | 3 | 6 | 15
LFSR 2
0 | 6 | 2 | 7 | 0
LFSR 3
9 | 7 | 6 | 5 | 4 | 3 | 1 | 1 | 0 | 3 | 5 | 7 | 7