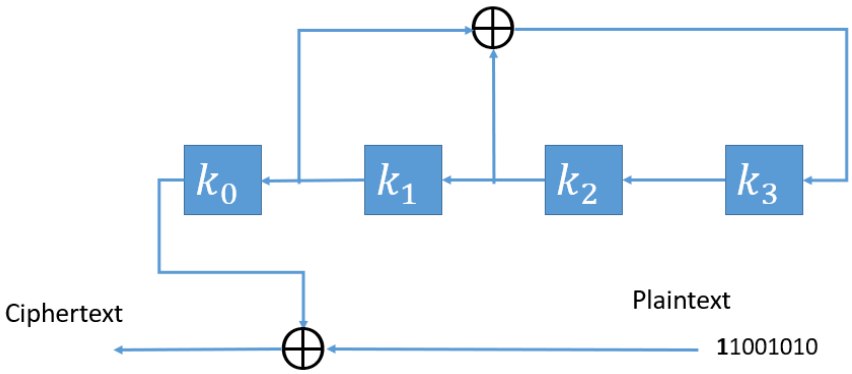
ISEC 2000 Fundamental Concepts of Cryptography
Laboratory 3
@ Computing, Curtin University

Notes:

- Make sure you complete prac questions. Assignments are highly related to them. In fact, programming questions are building blocks for the assignments.
- Group discussion is encouraged but make sure you complete questions individually.
- Ask questions not just answers. There is no answer of prac questions documented or provided for computing units.
- You can use your preferred programming language, C/C++, Java, or Python. Do NOT rely on libraries excessively.

1. Considering the following stream cipher with a Linear Feedback Shift Register (LFSR) as the random key generator. The initial state of the LFSR is given as $key = (k_0, k_1, k_2, k_3) = (1100)$. For a plaintext message $m = \mathbf{1}1001010$ (the bit in bold is the first bit), compute the corresponding ciphertext **step-by-step**.



2. The Euclidean Algorithm computes the greatest common divisor of two numbers, i.e., $gcd(a, b)$. The Extended Euclidean Algorithm computes not only the $gcd(a, b)$ but also the coefficients x and y such that:

$$ax + by = gcd(a, b). \tag{1}$$

For any numbers a, b, if we can compute $gcd(a, b), x, y$, how can we use it to calculate the inverse modulo $a^{-1} \bmod b$? (Hint: the inverse modulo $a^{-1} \bmod b$ is a number that satisfies $aa^{-1} \equiv 1 \bmod b$)

3. Please write a program to implement the Extended Euclidean Algorithm. Your program should take two numbers a, b as inputs and output the inverse modulo $a^{-1} \bmod b$ if it exists, otherwise print error message stating the value of $gcd(a, b)$ (which should not be 1).