1) The AES S-box is based on multiplicative inverses in the finite field of 256 elements. The irreducible polynomial \( x^8 + x^4 + x^3 + x + 1 \) is used in the construction.

(a) Develop the Galois LFSR that corresponds to this polynomial.

(b) Use the LFSR for finding the multiplicative inverse of \( X \) (which finite field element corresponds to the byte 02).

(c) Find multiplicative inverse of the finite field element that corresponds to the byte 10.

2) (a) Find a Fibonacci LFSR and its initial internal state such that
- there are 7 cells;
- feedback is from at least two cells;
- every second output bit is zero and the rest of output bits are ones.

(b) Find a Galois LFSR and its initial internal state such that
- there are 7 cells;
- feedback is to at least two cells;
- every second output bit is zero and the rest of output bits are ones.

3) We know that a Fibonacci LFSR has 6 cells and that it has produced the output stream (portion) of 011 111 000 010. Find the feedback structure of the LFSR.

4) For the Geffe generator, referring to lecture slides,

(a) Show that "Distribution of values \( b_i \oplus s_i \) is not uniform: zero appears with 75 \% frequency while one appears only with 25 \% frequency."

(b) Find out how much is "relatively often" in the following sentence: "Candidates were chosen in such way that each of the equalities \( s_i = b_i \) and \( s_i = c_i \) hold with around 75 \% frequency. Still, for a wrong candidate pair, \( b_i \neq s_i \neq c_i \) should occur relatively often."

5) The Ciphertext Feedback mode (CFB) for encryption works as illustrated in the figure below.

(a) Explain how decryption is done in the CFB mode.

(b) Assume you have several (physically implemented) instances of a block cipher function \( E \) and its inverse \( D = E^{-1} \) available.

Is it possible to parallelize encryption or decryption process in CFB mode?

(c) Same question as (b) but for (i) ECB (ii) CBC (iii) Counter mode?
6) Let us consider the toy-scale block cipher that is defined by the figure below. 

The block size is (pathetic) three bits while key size is (also pathetic) six bits which consists of three bits in Key1 and three bits in Key2.

We know that 000 is encrypted to 010 and 111 is encrypted to 001. Break the key by using "Meet-in-the-middle" attack.

\[\begin{array}{c|c|c|c}
\text{Input} & \text{Output} \\
0 & 4 \\
1 & 3 \\
2 & 5 \\
3 & 6 \\
4 & 1 \\
5 & 0 \\
6 & 7 \\
7 & 2 \\
\end{array}\]