Exercise 12. Besides the CBC mode, the CFB mode can be used for the generation of a MAC. The plaintext consists of the blocks $M_1, \ldots, M_n$, and we set the initialization vector $C_0 := M_1$. Now, we encrypt $M_2, \ldots, M_n$ in CFB mode with the key $K$, which results in the ciphertexts $C_1, \ldots, C_{n-1}$. For the MAC, we use $MAC_K := E_K(C_{n-1})$.

Show that this scheme results in the same MAC as the algorithm in example 10.5 from the lecture notes with the initial value set to $C_0 := 0$.

Exercise 13. Sign the message $m := 231$ using the ElGamal signature scheme. The parameters for the crypto system are:

$$p := 4793, x_A := 9177, a := 4792.$$ 

Before signing, check if these parameters fulfill the requirements of the signature scheme. Alternative values (in case the requirements are not fulfilled) are:

$$p := 8087, x_A := 257, a := 1400.$$ 

The random number is $k := 2811$.

Exercise 14. Verify the ElGamal signature $< r, s > := <373, 15>$ for the message $m := 65$. The message was signed using the public parameters $y_A := 399$, $p := 859$ and $a := 206$. 