Problem 1. *(CBC and CFB for MAC generation)* Both, the CBC mode and the CFB mode, can be used for the generation of a MAC as follows.

- A plaintext is divided into \( n \) equally-sized blocks \( M_1, \ldots, M_n \).
- For the CFB-MAC, the ciphertexts are \( C_i = M_{i+1} \oplus E_K(C_{i-1}) \) for \( i = 1, \ldots, n-1 \) and \( \text{MAC}_K^{(n)} = E_K(C_{n-1}) \) with initial value \( C_0 = M_1 \).
- For the CBC-MAC, the ciphertexts are \( \hat{C}_i = E_K(\hat{C}_{i-1} \oplus M_i) \) for \( i = 1, \ldots, n-1 \) and \( \hat{\text{MAC}}_K^{(n)} = E_K(\hat{C}_{n-1} \oplus M_n) \) with initial value \( \hat{C}_0 = 0 \).

Show that the equivalency \( \text{MAC}_K^{(n)} = \hat{\text{MAC}}_K^{(n)} \) holds.

Problem 2. *(Forging an ElGamal signature for arbitrary hashed messages with \( r \geq p \))* An attacker has intercepted one valid signature \((r, s)\) of the ElGamal signature scheme and a hashed message \( h(m) \) which is invertible modulo \( p - 1 \). Let \( h(m') \) any hashed message, \( u = h(m')(h(m))^{-1} \mod p - 1 \) and \( s' = su \mod p - 1 \).

Show that the attacker can generate a signature \((r', s')\) for the hashed message \( h(m') \), if \( 1 \leq r' < p \) is not verified.

Problem 3. *(Forging an ElGamal signature)* Let \( p \) be prime with \( p \equiv 3 \pmod{4} \), and let \( a \) be a primitive element modulo \( p \). Furthermore, let \( y = a^x \mod p \) be a public ElGamal key and let \( a \mid p-1 \). Assume that it is possible to find \( z \in \mathbb{Z} \) such that \( a^{gz} \equiv y^r \pmod{p} \).

Show that \((r, s)\) with \( s = (p-3)2^{-1}(h(m) - rz) \mod (p-1) \) yields a valid ElGamal signature for some \( r \) and a chosen message \( m \) with \( (h(m) - rz) \) is even.