1. (30 points) In class we learned about the ciphertext stealing trick to encrypt fragmentary data under CBC. Describe how to use this to encrypt a message that is shorter than \( n \) bits, where \( n \) is the block length of the blockcipher. Draw a picture to illustrate your ideas.

2. (60 points) Fix a blockcipher \( E : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}^n \) and let CBCMAC\(_K\)(\( M \)) be the CBC MAC, using \( E_K \), of a message \( M \) that is a positive multiple of \( n \) bits. We have seen that this construction is not secure as a (variable-input-length) MAC. So consider instead the proposal

\[
\text{CBCMAC2}_{K, K'}(M) = \text{CBCMAC}(M) \oplus K'
\]

where \( K, K' \in \{0, 1\}^n \).

Show that CBCMAC2 is a bad MAC, too: you can easily break the MAC security of CBCMAC2. Analyze the advantage of your attack.

3. (60 points) CBC-Chain is a stateful blockcipher-based mode of operation that was actually used in SSH. To encrypt, we use CBC with an IV that is the last ciphertext block produced from the prior encryption. Initially, the IV is a random string. Give an attack that breaks the left-or-right security of CBC-Chain[\( E \)] and analyze its advantage.