Security of EMAC

1. Recall what is a MAC, what it is used for, and what is the threat model.
2. Recall how CBCMAC works.
3. Recall how to do a chosen message forgery attack on CBCMAC. What is the complexity of the attack? (Assume it is based on DES.)
4. We consider EMAC based on DES encryption. We use a key $K = (K_1, K_2)$ where K_1 is a key for CBCMAC based on DES and K_2 is a DES key. We define

   $$\mathsf{EMAC}_K(x) = \mathsf{DES}_{K_2}(\mathsf{CBCMAC}_{K_1}(x))$$

   Show that we can run a efficient key recovery attack with a few known messages. What is the complexity?
5. Show that we can exploit collisions on EMAC to adapt the attack on CBCMAC. What is the complexity?
6. How to conclude on the security of EMAC?