Cryptology: Problem Sheet 4

Topic: IND-CCA Security and Authenticated Encryption

1. Mount CCA-attacks on CBC, OFB and Counter Mode of operations.

2. Let F be a strong pseudorandom permutation, and define the following fixed-length encryption scheme: On input a message $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a uniform $r \in \{0,1\}^{n/2}$ and computes $c := F_k(m\|r)$. Prove that this scheme is CCA-secure, but not an authenticated encryption scheme.

3. Let $(\mathsf{KG}_E, \mathsf{Enc}, \mathsf{Dec})$ be a IND-CPA secure randomized encryption scheme. Let $(\mathsf{KG}_M, \mathsf{TG}, \mathsf{Vrfy})$ be a EUF-CMA secure MAC. Consider the following Encrypt-then-MAC type derived cipher $\Pi := (\mathsf{KG}, \mathsf{AE}, \mathsf{VD})$, where

   $$\mathsf{AE}_{K_1,K_2}(m) := \{(r,c) \leftarrow \mathsf{Enc}_{K_1}(m),\ t \leftarrow \mathsf{TG}_{K_2}(c),\ \text{return } (r,c,t)\}.$$

   Prove that the authenticated encryption is not secure. How can you justify your answer? [Note that we know the following result: "Encrypt-then-MAC achieves secure AE given that the underlying Encryption and MAC schemes are secure."]