Cryptology: Problem Sheet 3

Topic: Modes of Operation and Message Authentication Code

1. Consider a CBC-mode encryption is used with a 128-bit PRF having a 256-bit key to encrypt a 1024-bit message. What would be the length of the resulting ciphertext?

2. Let F be a pseudorandom function mapping 128-bits to 128-bits. Consider the mode of operation in which a uniform value $r \leftarrow_{\$} \{0,1\}^{64}$ is chosen, and the i-th ciphertext block c_i is computed as
$$c_i := F_k(r\|i) \oplus m_i.$$
What is the maximum message length that can be encrypted using this scheme? Does this scheme have indistinguishable encryptions in the presence of an eavesdropper.

3. Let F be a pseudorandom function. Show that each of the following MACs is insecure, even if used to authenticate fixed-length messages. (In each case Gen outputs a uniform $k \in \{0,1\}^n$. Let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i.)
   (a) To authenticate a message $M = M_1\|M_2\|\cdots\|M_\ell$, where $M_i \in \{0,1\}^n$, compute the tag $t := F_k(M_1) \oplus \cdots \oplus F_K(M_\ell)$.
   (b) To authenticate a message $M = M_1\|M_2\|\cdots\|M_\ell$, where $M_i \in \{0,1\}^{n/2}$, compute the tag $t := F_K(\langle 1 \rangle\|M_1) \oplus \cdots \oplus F_K(\langle \ell \rangle\|M_\ell)$.
   (c) To authenticate a message $M = M_1\|M_2\|\cdots\|M_\ell$, where $M_i \in \{0,1\}^n$, choose uniform $r \leftarrow \{0,1\}^n$ and compute $t := F_K(r) \oplus F_K(M_1) \oplus \cdots \oplus F_K(M_\ell)$, and let the tag be (r,t).

4. Consider the message authentication code where the tag generation function $\mathsf{TG} : \{0,1\}^k \times \{0,1\}^{2(n-1)} \to \{0,1\}^n$ is given by
$$\mathsf{TG}_K(x_1,x_2) = F_K(0\|x_1) \oplus F_K(1\|x_2),$$
where F is a PRF. Mount an existential forgery attack on it. Can you extend this attack to mount an universal forgery attack against the function?

5. Suppose you are given two MAC systems $\mathsf{MAC}_1 = (\mathsf{KG}_1, \mathsf{TG}_1, \mathsf{Vrfy}_1)$ and $\mathsf{MAC}_2 = (\mathsf{KG}_2, \mathsf{TG}_2, \mathsf{Vrfy}_2)$. Define $\mathsf{MAC} = (\mathsf{KG}, \mathsf{TG}, \mathsf{Vrfy})$, where $\mathsf{KG}(1^n) = (\mathsf{KG}_1(1^n), \mathsf{KG}_2(1^n))$,
$$\mathsf{TG}((K_1,K_2),m) \;=\; \mathsf{TG}_1(K_1,m)\|\mathsf{TG}_2(K_2,m).$$
Vrfy is defined in the obvious way: on input $((k_1,k_2),m,(t_1,t_2))$, V accepts iff both $V_1(k_1,m,t_1)$ and $V_2(k_2,m,t_2)$ accept. Show that MAC is secure if either MAC_1 or MAC_2 is secure.