11 Security II (MGK)

(*a*) Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a private-key encryption scheme that operates on fixed-length messages from $\mathcal{M} = \{0,1\}^m$. Briefly explain a game that a user $\mathcal{U}$ of Π must be able to win against any polynomial-time adversary $\mathcal{A}$ with probability $\frac{1}{2} - \epsilon$ (where is ϵ is "negligible" with growing key length) for Π to be able to claim to offer "indistinguishable multiple encryptions under chosen-plaintext attack" (CPA security). [8 marks]

(*b*) Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a private-key encryption scheme that offers CPA security and operates on fixed-length messages $M \in \mathcal{M} = \{0,1\}^m$ with keys $K \in \mathcal{K} = \{0,1\}^\ell$. We use it to construct a new encryption scheme $\Pi' = (\mathsf{Gen}, \mathsf{Enc}', \mathsf{Dec}')$. In which of the following cases is Π' also CPA secure? Explain your answer. [2 marks each]

(*i*) $\mathsf{Enc}'_K(M) = \mathsf{Enc}_K(M \oplus 1^m)$

(*ii*) $\mathsf{Enc}'_K(M) = \mathsf{Enc}_K(M) \| \mathrm{LSB}(M)$

(*iii*) $\mathsf{Enc}'_K(M) = \mathsf{Enc}_K(M) \| \mathrm{LSB}(K)$

(*iv*) $\mathsf{Enc}'_K(M) = \mathsf{Enc}_{0^\ell}(M)$

[*Note:* LSB outputs the least significant bit of its input word, $\|$ is concatenation.]

(*c*) While reviewing an implementation of AES-CBC, you discover that it simply uses the last ciphertext block from the previously encrypted message as the IV value C_0 for encrypting the next message. The implementation's author argues that as long as the IV of the very first message was chosen uniformly at random, all resulting subsequent ciphertext blocks will also be distributed uniformly at random, and therefore make good IVs. Why is this construction nevertheless not CPA secure? [4 marks]