5 Cryptography (mgk25)

(*a*) Consider the following two alternative definitions of a MAC function, which receives as input an $(n \cdot L)$-bit long message of the form $M = M_1 \| M_2 \| \ldots \| M_L$ with $M_i \in \{0,1\}^n$ and a private key $K \in \{0,1\}^n$ picked uniformly at random, returning a tag $T \in \{0,1\}^n$. Show how neither definition provides the security property of *existential unforgeability*.

(*i*) Let F be an n-bit to n-bit pseudo-random function. Return the message tag $T = F_K(M_1) \oplus F_K(M_2) \oplus \cdots \oplus F_K(M_L)$. [4 marks]

(*ii*) Let F be a $(2n)$-bit to n-bit pseudo-random function. Return the message tag $T = F_K(\langle 1 \rangle \| M_1) \oplus F_K(\langle 2 \rangle \| M_2) \oplus \cdots \oplus F_K(\langle L \rangle \| M_L)$. [6 marks]

[*Notation:* $\|$ = concatenation of bit strings, $\oplus$ = bit-wise XOR, $\langle i \rangle$ = n-bit binary representation of non-negative integer i.]

(*b*) Your colleague proposes to construct an authenticated encryption scheme that encrypts a plain-text message M by first calculating the message authentication code $\mathrm{CMAC}_K(M) = T$, and then forms the ciphertext by encrypting $M \| T$ using CFB mode with initial vector $IV = E_K(T)$, using the same key and blockcipher E_K. Does this construction offer CCA security? Why or why not? [5 marks]

(*c*) Given a block cipher E_K with n-bit block size, where $n \geq 64$ is a power of two, how can you use E_K to construct a strong pseudo-random permutation for $\frac{n}{2}$-bit blocks? [5 marks]