8 Security I (MGK)

(*a*) In the Galois field GF(2^8) modulo $x^8 + x^4 + x + 1$, calculate

(*i*) the difference 1100 1010 minus 1001 0011; [2 marks]

(*ii*) the product 0100 1011 times 0000 1001. [6 marks]

(*b*) Briefly explain two advantages that arithmetic in GF(2^{128}) has over arithmetic in $\mathbb{Z}_{2^{128}}$ when designing cryptographic algorithms. [6 marks]

(*c*) Given a block cipher E_K and a corresponding decryption function D_K, provide a formula for the decryption of the following modes of operation and state for each whether the E_K or D_K calculations required during decryption can be executed in parallel: CBC, OFB, CTR. [6 marks]