6 Cryptography (mgk25)

(*a*) (*i*) Choose and briefly describe one major application of elliptic-curve group operations in cryptography. [4 marks]

(*ii*) What other group operation was previously (and still is) widely used for the same purpose? [2 marks]

(*iii*) What is a major advantage of elliptic curve group operations over the group operation you named in Part (*a*)(*ii*)? [4 marks]

(*b*) In the Galois field GF(2^8) modulo $x^8 + x^4 + x^3 + x^2 + 1$, calculate

(*i*) the sum 0011 1001 plus 0110 1100; [2 marks]

(*ii*) the product 0100 1011 times 0000 1001. [4 marks]

(*c*) In Lamport's one-time password scheme, the user is given a list of passwords $R_n, \ldots, R_0$ generated using the following algorithm:

$R_0 \leftarrow$ random
for $i := 1$ **to** n
    $R_i := h(R_{i-1})$

(*i*) State two properties required of function h. [2 marks]

(*ii*) Complete the password verification algorithm implemented in the server by filling in the ellipses (...) below:

$Q := \ldots$
while true
    $P :=$ read password
    if ...
        ...
        grant access
    else
        deny access

[2 marks]