

## 2003 Paper 8 Question 6

### Security

- (a) The Digital Signature Standard is computed using the following equations:

$$r = (g^k \bmod p) \pmod{q}$$
$$s = (h(M) - xr)/k \pmod{q}$$

Describe what the various symbols represent. [4 marks]

- (b) Write down the equation(s) used to verify a signature. [4 marks]
- (c) The standard specifies that  $r$  must lie strictly between 0 and  $q$ . What might go wrong if an implementation does not check this? [4 marks]
- (d) A designer decides to economise on code size by omitting the hash function computation, that is, replacing  $h(M)$  by  $M$ . What are the consequences of this optimisation? [8 marks]