Security part 2 Second Question 2003 p8q6
RJA

The Digital Signature Standard ~~assumes~~ 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)

Write down the equation(s) used to verify a signature (4 marks)

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)

A designer decides to economise ~~on~~ 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)

Answers

First and second: bookwork

Third: $r = 0$ or q makes signatures degenerate + thus forgeable

Fourth: Can forge signature on M' for $M' - M = nq$ for any existing signature on M.