2008 Paper 7 Question 9

Security

(*a*) What does it mean for a hash function to be *collision-resistant*, and to be *preimage-resistant*? [4 marks]

(*b*) The current scheme for doing background checks on schoolteachers, health service staff and others who have contact with children is too slow, and your job is to design its replacement. You are given a database of 20,000 convicted sex offenders stored as (date of birth, name). You may not release any information that might identify an offender. You may only release signed information providing evidence that a supplied input of (date of birth, name) does not appear on the offenders' database. Finally, because there are huge peaks in transaction volume at the start of the school year and when National Health Service staff rotate jobs, you want all – or almost all – digital signatures to be precomputed for performance reasons.

Provide an outline design for the system and show how it meets the requirements. [16 marks]