2007 Paper 8 Question 11

Security

(*a*) In cryptography, what do we mean when we describe a hash function as a "pseudorandom function"? [4 marks]

(*b*) A hash function h is said to be *collision resistant* if it is hard to find $m_1 \neq m_2$ such that $h(m_1) = h(m_2)$ and *preimage resistant* if given a random y it is hard to find X such that $h(X) = y$.

Describe how hash functions can be used in the following applications, in each case indicating whether the function needs to be collision-resistant or preimage-resistant.

(*i*) digital certificates generated by a trustworthy CA for use in SSL/TLS; [4 marks]

(*ii*) the exchange of electronically-signed contracts by companies; [4 marks]

(*iii*) computing fingerprints on "known good" files by anti-virus software; [4 marks]

(*iv*) hash chains of digital coins for use in an electronic cash system. [4 marks]