1998 Paper 7 Question 9

Security

Describe the purpose of hash functions, message authentication codes and digital signatures, sketching a possible construction for each of them. [12 marks]

A funds transfer system authenticates messages between its member banks by having the sending and receiving banks compute a MAC on each message using a key which each pair of correspondent banks in the system establishes monthly using public key techniques. The sending bank then computes a digital signature on the MAC using a long-term signing key.

If the MAC is 32 bits long, is this arrangement more, or less, secure than signing a 128-bit hash of the message, and why? [5 marks]

To what extent would matters be changed if all messages handled by the system were logged by a trusted third party? [3 marks]