9 Security I (MGK)

(*a*) Name and briefly explain *three* increasingly demanding security properties expected from a *secure hash function h*. [3 marks]

(*b*) Explain how a 128-bit secure hash function h can be used to implement a one-time signature scheme, *and* how to verify such a signature. [5 marks]

(*c*) The T1000 encryption module was designed to make *TeleGroove* messages difficult to read for eavesdroppers. Such messages are character sequences of arbitrary length, encoded using a 5-bit alphabet $A = \{a_0, \ldots, a_{31}\}$. The T1000 module reads blocks of up to 1000 characters at a time into its memory $(m_0, m_1, \ldots, m_{999})$ and then outputs them again in a different order $(m_{K(0)}, m_{K(1)}, \ldots, m_{K(999)})$, according to a secret key table $K : \{0, \ldots, 999\} \rightarrow \{0, \ldots, 999\}$ that is shared with the respective recipient of each message. It repeats that process until the block ending with the last character has been processed.

(*i*) What constraint on K ensures that no information is lost? [2 marks]

(*ii*) Identify an ambiguity in the above description and propose a flaw hypothesis regarding a related residual-information vulnerability in this device. [4 marks]

(*iii*) What is the smallest number of blocks that a chosen-plaintext attacker has to send through the device to recover K? Give an example of the content of such blocks and explain how to recover K from them. [6 marks]