4 Cryptography (mgk25)

(*a*) List *six* properties that an algebraic group should have to be usable for Diffie–Hellman key exchanges. [6 marks]

(*b*) Let $T : A^8 \to A^4$ be a new collision-resistant compression function approved for use in Tripos papers, where $A = \{\mathtt{a}, \ldots, \mathtt{z}, \mathtt{0}, \ldots, \mathtt{9}, \mathtt{=}, \mathtt{\&}\}$ is the "base38" alphabet used.

(*i*) Assuming a Tripos student with pocket calculator can evaluate T once per minute, and assuming all students have a brain with unlimited memory and instantaneous recall time, how many hours will it roughly take until at least half of all students can be expected to each have independently found a collision $T(x) = T(y)$ with $x \neq y$? [2 marks]

(*ii*) Use T to define a collision-resistant hash function $H : A^* \to A^4$, such that the security proof for the Merkle–Damgård construction can be applied. Describe your padding scheme and list the input blocks fed into T when you evaluate $H($"`love&peace`"$)$. [6 marks]

(*iii*) Consider an ATM that receives from a bank computer authorization responses of the form (M, C), such as

$$M = \text{“}\mathtt{txn=491\&pincheck=0\&limit=0}\text{”}, \quad C = H(K \| M)$$

where $K \in A^8$ is the private key shared between the bank and the ATM, and H is as in Part (*b*)(*ii*).

After recalculating and checking C, the ATM splits M into fields separated by "`&`", and then executes any variable assignments it encounters in such fields from left to right, ignoring fields that do not form an assignment. The above M confirms that the PIN provided for transaction 491 was incorrect and that the cardholder is therefore authorized to receive up to £0 in cash.

Mallory has intercepted the line between the ATM and the bank computer and can read (M, C) and replace it with a modified message (M', C'). She would like to withdraw cash without knowing the PIN. Show how she can form a message M' that ends in "`&pincheck=1&limit=1000`" and how she can calculate for that M' a matching tag $C' = H(K \| M')$ without knowing K. [6 marks]