5 Software and Security Engineering (rja14)

The basic Europay-MasterCard-VISA transaction flow is

$$\begin{array}{ll} C \longrightarrow T: & PAN, d_1, \mathrm{Cert}_{KB}(PAN, d_1) \\ T \longrightarrow C: & N, t, X, d_2, PIN \\ C \longrightarrow T: & d_3, \mathrm{MAC}_{KCB}(d_3, T, N, t, X) \end{array}$$

where C is the customer card, T the merchant terminal, d_1 the card data, PAN the primary account number, N the unpredictable number, t the date, X the amount, d_2 and d_3 the merchant data, KB the bank signing key, KCB the key shared between the bank and the card and PIN the customer PIN.

(*a*) How does the merchant terminal obtain authorisation from the card-issuing bank? [4 marks]

(*b*) Describe two attacks on this protocol that can be used to commit fraud. In each case describe the protocol flaw or system limitation responsible. [8 marks]

(*c*) You are a security engineer working for a payment network owned by a country's banks. Which of the two attacks would most worry you, and what would you do to forestall or mitigate it? [8 marks]