4 Cryptography (mgk25)

A building access-control smartcard uses the following authentication protocol. Let G be a generator for an elliptic-curve based cyclic group $(E(\mathbb{Z}_p, a, b), +)$ of order q. The card stores in its non-volatile memory a secret key $u \in \mathbb{Z}_q^*$ and a public card identifier $U := uG$. The door does not know u. Curve parameters were chosen such that determining u from curve point U is computationally infeasible.

When the user holds the contactless card in front of the door reader, the card picks a number $c \in \mathbb{Z}_q^*$ and the door picks a number $d \in \mathbb{Z}_q^*$, both uniformly at random. The card calculates the coordinates of elliptic-curve point $C := cG$.

They then exchange the following three messages:

card		**door**
read u, U from memory		
pick $c \in \mathbb{Z}_q^*$, $C := cG$	① $\xrightarrow{(U, C)}$	
	② $\xleftarrow{d}$	pick $d \in \mathbb{Z}_q^*$
$r := (c + du) \bmod q$	③ $\xrightarrow{r}$	

(a) What checks should the door perform on the received values U, C, r to verify that the card identified by U really is in possession of u? [4 marks]

(b) How many bits will be required to encode the values exchanged in these three messages in order to achieve a security level similar to the use of a 128-bit key in a symmetric MAC? [4 marks]

(c) Your colleague is concerned that the calculation of $C := cG$ in the card slows down the authentication process too much, and therefore proposes to postpone transmission of C to the third message, i.e. to change the three protocol messages from previously (U, C), d, r to now U, d, (C, r). Would this affect security? [5 marks]

(d) Due to supply-chain issues, the hardware manufacturer no longer can make door readers that send data to the card. Modify the original protocol such that only the card sends data to the door. The card maintains a counter m for how often it has been used, and the door remembers the highest value of m it has previously seen and will only open again when presented with a new value m higher than any seen before. Instead of receiving d in message ②, let the card calculate d in a way such that the card provides a digital signature of m, and sends (d, m) to the card. Keep message ③ the same. [5 marks]

(e) Which value appearing in the original protocol no longer has to be transmitted by the unidirectional variant from Part (d), and why? [2 marks]