4 Cryptography (mgk25)

(*a*) Consider a cyclic group $(\mathbb{G}, \bullet)$ of order q with generator g.

Briefly explain the difference between the Computational Diffie–Hellman problem and the Decision Diffie–Hellman problem for $\mathbb{G}$, and state how if one of these problems is hard for $\mathbb{G}$, what this implies for the other. [6 marks]

(*b*) While decompiling the executable of an ECDSA implementation with unknown domain parameters, you encounter a prime-number constant of the form

```
0x ffffffff ffffffff fffffffe 0626bd0c 2f33945b 7d67dbcb
```

Based on the structure of its hexadecimal representation, what rôle could this number play? Explain your answer based on how elliptic-curve groups used in cryptography can be constructed. [6 marks]

(*c*) A certification authority C would like to issue certificates that bind a user A's public key PK_A to not just that user's name, but to 10 different personal attribute values $A_0, \ldots, A_9$, e.g. forename, surname, year of birth, birthday, gender, country, postcode, street address, email, portrait photo. User A can then use such a certificate to register with a range of different online services. However, not all attributes are required, or even appropriate, to be revealed to each service: some may only need the email address, whereas others need perhaps only forename, year of birth, gender, and the photo.

User A should, therefore, be able to choose, which subset $S \subset \mathbb{Z}_{10}$ of these 10 attributes they want to reveal each time they present their certificate to a service. One solution would be that C signs for each user 2^{10} different certificates, each including a different subset of attributes. But that would be rather inefficient.

Propose a certificate format, where C generates just one digital signature for each user A, but A then can modify their certificate to remove any subset of the ten attribute values, such that the recipient still can be sure the received attribute values are authentic, while not being able to infer the value of the removed attributes (except with negligible probability in polynomial time). Explain in detail what A receives from the certification authority, and what A provides to a service that only needs a certificate covering attribute subset S. [8 marks]