d) No, it is not safe as Fixed-Diffie Hellman is used after the key has been compromised.

e) No, it is not safe because of weak session key and usage of Fixed-Diffie Hellman.

5) (Programming) Discrete Log Meet-in-the-Middle Attack [6 points].

b) No, it does not present a problem for practical instantiation of the discrete log problem, rather it reduces it by a fraction.

c) In order to minimize the costs of the attack, we could pre-compute ~~the table~~ a smaller table and do more lookups visited.