3 Cryptography (mk428)

(*a*) Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme that offers CCA security. Explain the concept of *forward secrecy*, why it might be useful, and why Π does not offer it. [3 marks]

(*b*) Explain how the Diffie–Hellman key exchange works, and the assumptions under which it is secure. [3 marks]

(*c*) You and your colleague are asked to design a payments system based on an authenticated symmetric encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$, a digital signature scheme $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$, a Diffie–Hellman group with generator g, and a key derivation function KDF. The requirements are as follows:

- Let B be a bank, and let Alice (A) be a customer of B. Say A has a digital token T (which we take to be an arbitrary bit string) that is worth money. A can deposit that money in her account by securely sending T to B.
- You may assume that the bank knows the public keys of all of its customers, and that each customer knows the public key of the bank.
- As the token T is sent over the network, it must be kept confidential from active attackers. Moreover, the protocol must provide forward secrecy.

Let $(PK_A, SK_A) \leftarrow \mathsf{Gen}$ be Alice's signature keypair, and $(PK_B, SK_B) \leftarrow \mathsf{Gen}$ be the bank's keypair. Your colleague proposes using the following scheme:

$B \to A:\ (g^x, \mathsf{Sign}_{SK_B}(g^x))$

A receives (g^x, S) and checks whether $\mathsf{Vrfy}_{PK_B}(g^x, S) = 1$.
If this succeeds, A calculates $K = \mathsf{KDF}((g^x)^y)$ and sends:

$A \to B:\ (g^y, \mathsf{Sign}_{SK_A}(g^y), A, \mathsf{Enc}_K(T))$

B receives (g^y, S, N, C) where N is a customer name, looks up N's public key PK_N, and checks that $\mathsf{Vrfy}_{PK_N}(g^y, S) = 1$; if successful, B decrypts $\mathsf{Dec}_{\mathsf{KDF}(g^{xy})}(C) = T$ and credits it to the account belonging to N.

Let Mallory (M) be an active adversary who is also a customer of the bank. Show that your colleague's scheme is not secure: when Alice wants to deposit a token T in her account, M can cause his account to be credited instead. [7 marks]

(*d*) Suggest an alternative protocol that meets the requirements in part (*c*) while avoiding the problems in your colleague's scheme, and briefly justify your design. [7 marks]