3 Cryptography (mk428)

(a) Let \( \Pi = (\text{Gen}, \text{Enc}, \text{Dec}) \) be a public-key encryption scheme that offers CCA security. Explain the concept of forward secrecy, why it might be useful, and why \( \Pi \) 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 \((\text{Enc}, \text{Dec})\), a digital signature scheme \((\text{Gen}, \text{Sign}, \text{Vrfy})\), a Diffie–Hellman group with generator \( g \), and a key derivation function \( \text{KDF} \). 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 \((\text{PK}_A, \text{SK}_A) \leftarrow \text{Gen}\) be Alice’s signature keypair, and \((\text{PK}_B, \text{SK}_B) \leftarrow \text{Gen}\) be the bank’s keypair. Your colleague proposes using the following scheme:

\[
B \to A : (g^x, \text{Sign}_{\text{SK}_B}(g^x))
\]

\( A \) receives \((g^x, S)\) and checks whether \( \text{Vrfy}_{\text{PK}_B}(g^x, S) = 1 \).

If this succeeds, \( A \) calculates \( K = \text{KDF}((g^x)^y) \) and sends:

\[
A \to B : (g^y, \text{Sign}_{\text{SK}_A}(g^y), A, \text{Enc}_K(T))
\]

\( B \) receives \((g^y, S, N, C)\) where \( N \) is a customer name, looks up \( N \)’s public key \( \text{PK}_N \), and checks that \( \text{Vrfy}_{\text{PK}_N}(g^y, S) = 1 \); if successful, \( B \) decrypts \( \text{Dec}_{\text{KDF}(g^{xy})}(C) = T \) 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]