**H0N21A Introduction to ICT Security** **Bart Preneel** Model question 2

**Name:** ____________________________ **Year:** ______________

Consider the following variant of the Boyd and Mathuria protcol with as goal to protect the communication between a mobile device and an access point.

**Alice** $A$ **Bob** $B$

$$\xrightarrow{\quad A||N_A \quad}$$

$$\xleftarrow{\quad E_{P_A}(k \,||\, N_B \,||\, certB) \,||\, E_k(B||N_B) \,||\, \mathrm{Sig}_B(h(B||N_B||k||P_B)) \quad}$$

$$\xrightarrow{\quad E_k(N_A \,||\, N_B) \quad}$$

One has the following definitions:

- $A$ the identity of Alice and $B$ the identity of Bob
- $N_A$ a nonce generated by Alice
- $h(.)$ a collision resistant hash function
- $E_k(.)$ symmetric encryption with the secret key $k$
- $E_{P_X}(.)$ encryption with the public key $P_X$ of $X$
- $\mathrm{Sig}_X(.)$ signature with the private key $S_X$ of $X$
- $certX$ a certificate of a third party on the public key of $X$

**a)** Discuss briefly the three steps in the protocol and their roles (you do not need to write down all the details – an oral explanation is sufficient).

**b)** Which goals are achieved by this protocol: entity authentication, implicit key authentication, key confirmation, explicit key authentication, anonymity w.r.t. third parties, key control, key freshness – both for Alice and for Bob. Explain why.

**c)** Does this protocol offer forward secrecy and is it resistant against a known key attack? Explain why.

**d)** If all the properties under b) are not met: modify the protocol so that these properties are met. Try to use as few steps as possible and do not introduce new cryptographic algorithms unless they are absolutely necessary.