National University of Singapore
School of Computing

CS2105 **Problem Set 6** Semester 2 13/14

1. Suppose Alice wants to send a secure email m to Bob, and wants to ensure confidentiality, sender authentication, and message integrity. Alice performs the following steps (See Figure 8.21):

    1. generates a random session key K_s
    2. encrypts the session key K_s with Bob's public key, K_B^+, obtaining $K_B^+(K_s)$
    3. hashes the message m with a cryptographic hash function H, obtaining $H(m)$
    4. encrypts the hash with Alice's private key K_A^-, obtaining $K_A^-(H(m))$
    5. encrypts the message m, concatenated ($\oplus$) with $K_A^-(H(m))$, using the session key K_s, obtaining $K_s(m \oplus K_A^-(H(m)))$
    6. finally, sends $K_s(m \oplus K_A^-(H(m))) \oplus K_B^+(K_s)$ to Bob

    Show what Bob has to do to verify that m is indeed from Alice and has not been modified.

    Explain how these steps ensure confidentiality (prevents eavesdropping), sender authentication (prevents impersonation of Alice), and message integrity (prevents tempering with m), with the help of a certification authority.

2. A certificate issued by a certification authority (CA) is digitally signed. To verify the digital signature of the CA, however, the public key of the CA is needed. How can we know that the given public key of a CA is trustable?

3. Ah Kow goes to the website www.ura.gov.sg to pay his parking fines to URA over unsecure HTTP. When he clicks the "pay" button on the website, he is redirected to a website www.paymenow.com, which runs HTTPS and asks for his credit card number. The certificate for www.paymenow.com is properly signed by Verisign. Should Ah Kow give his credit card number? Why or why not?

4. The School of Computing's VPN runs over SSL instead of IPSec. What are the advantages of running a VPN over SSL versus over IPSec?