**COMP7906A Cyber Security**

**Assignment 3**

**(Due on Nov 12, 23:59)**

**Q1.**

Find the public key certificate (PKC) of [www.google.com](http://www.google.com) in your computer’s browser.

1. Screen capture the display of the PKC of your browser.
2. Who is the CA that issue the PKC?
3. What is the signing algorithm and what is the length of the key that signed the PKC?

**Q2.**

(1) Alice uses RSA public key encryption system and her public key is (eA, nA) = (23, 77), what is Alice’s private key (dA, nA)?

(2) If Bob’s public key is (eB, nB) = (5, 91) and private key is (dB, nB) = (29, 91), Alice uses Bob’s public key to encrypt a message m and the ciphertext c is 10, decrypt c and get the value of the plaintext m.

**Q3.**

The following schema illustrates how A sends a signed and encrypted message to B.



1. Suppose A sent a message to B yesterday. Today, A denies that he had sent the message before. How can B show evidence to a third party that A had sent the message before?
2. How can B be sure that another person D cannot see the content of the message, even if D knows the cipher-text in transmission?
3. In generating the digital signature, the cryptographic hash value of the Mesg is computed and then signed. Which properties do you require from the cryptographic hash function to prevent an attacker from forging the signature?

**Q4.**

Following states four different ways of sending a signed-and-encrypted message M from A to B, where Xprv(D) is using the private key of X to process the data D, Xpub(D) is using the public key of X to process data D, H(M) is the hash value of M, and Ek(D) is using the symmetric block encryption key k to encrypt data D:

1. A sends Aprv(Bpub(M)) to B
2. A sends Aprv(H(M)), Bpub(M) to B
3. A sends Aprv(H(M)), Bpub(H(M)) to B
4. A sends Aprv(H(M)), Bpub(K), Ek(M) to B
5. Which of the above approach is wrong? Explain your answer.
6. Given that M is megabytes-long message. Block cipher encryption is faster than public key operations. For the remaining three correct ways, which one is most efficient? Which one is least efficient? Explain your answer.

**Q5.**

Given a modular exponentiation algorithm for n-bit integers that needs about n3 operations, how much does performance deteriorate by moving from 1024-bit to 2048-bit RSA?

**Q6.**

Design an e-payment protocol based on Needham and Schroeder Protocol for the following scenario. The e-commerce shop allows users to purchase items through the Internet. You can assume the communication between any 2 parties is secure. At the end of a shopping session, the shop will calculate the total cost of the purchase based on items in the user’s shopping cart. The user is then requested to pay the amount to the shop’s banking account. You are required to design a payment protocol such that:

(1) The bank does not know what items are purchased by the customer.

(2) The shop does not know how the customer make the payment, e.g. the bank account details of the customer.

(3) At the end of the payment, the user should have a proof that he has paid the specified amount into the shop’s banking account.

(4) The bank does not need to communicate with the shop directly during the process of payment.

You can assume that the shop has an account with the bank. The customer can make a payment into the shop’s bank account either using his bank account or any other payment method. You can also assume that secret keys are available between the following parties:  
 (i) The shop and the bank (Kshop)  
 (ii) The customer and the bank (Kcust)  
  
  
Show your designed protocol and explain how the above four requirements are satisfied.

Graphical user interface

Description automatically generated

|  |  |
| --- | --- |
| Action | Details |
| 1 | Customer (C) selects items (I) and confirm the order (O), and send the request  purchase(C,I,O) to the shop |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Q7.**

A group of around 20 persons wants to start a Web-based discussion forum.

(1) Each member will post some documents (mainly text) for other members to view and download. Yet other members cannot modify the document content. The member who posted the document is called the owner of the document.

(2) Members can post comments to those posted documents. Each comment is associated with one posted document, or can be a follow-up comment to another one.

(3) The documents are divided into three classes. One is ‘general’ (Class G), which can be seen by non-members as well. Another is ‘confidential’ (Class C), which can only be viewed by members. The third one is ‘selectively-confidential’ (Class S), which means only a set of selected members can view and comment on this document.

* The owner will decide the class of the document when it is posted. For a Class S document, the owner will also decide the list of member that can view/select this document.

(4) Similar to point (3), comments are divided into Class G, C, or S, using the following rules.

* A comment to a Class S document must be Class S. The set of selected members of the comment is the same as that of the document.
* A follow-up comment of a Class S comment must also be Class S. The set of selected members is unchanged.
* A comment to a Class C document is Class C.
* A follow-up comment of a Class C comment must also be Class C.
* Class of a comment to a Class G document will be decided to be G, C, or S when it is posted by the member who posted the comment. In case of a Class S comment, the list of members will also be selected by the member who posted this comment.

The discussion forum project decides to use cryptography to protect the data. This means all Class C or S documents/comments will be encrypted with some key, and decryption keys will be issued to members.

You are the designer of this project and is required to design a system to solve this problem. You need to focus on the cryptographic operations and key management issues, and can be very brief in describing the use of network/Internet technology.

As this is an open-ended question, you can state any additional assumptions as you prefer. In particular, you can change or add new rules about the document/comment classes. But you must give justifications.