COMP3355 Cyber Security

Assignment 2

(Due on Oct. 8, 23:55)

Q1. (10%)

Find the public key certificate (PKC) for www.google.com in your computer's browser.

1. (3%) Screen capture the display of the PKC of your browser.
2. (3%) Who is the CA that issue the PKC?
3. (4%) What is signing algorithm and what is the length of the key that signed the PKC?

Q2. (20%) [Programming with "big" numbers]

For your information, you might need to import some package to hold the "big" integer depending on different programming language you use. Only built-in packages are allowed. Java and python recommended.

(1) (5%) Implement a function that check if a "big" integer is a prime number or not. Your function must take in a string type parameter, which is the string of the "big" integer for checking. Your function will need to print out the result.
Do NOT use the probabilistic algorithm. Test your program and find the biggest number that you can check within 10 minutes on your PC.
E.g. prime for testing: 71755440315342536873
Function header example (java): **void isPrime(String str) {}**
You may not need to specify parameter type in python, but it must handle String well.

(2) (15%) Implement the Extended Euclid Algorithm which computes the inverse of c mod n, where c and n are "big" integers. Your function must take in two string parameters, first representing the string of c and the second representing the string of n. Your function will need to print out the result.
E.g. data for testing, c = 20999311111111111135, n = 33332322667876, result = 13204983474883
Function header example (java): **void inverseMod(String stringC, String stringN) {}**
You may not need to specify parameter type in python, but it must handle String well.

Please follow the requirement of how to define your program, otherwise you may lose all your points for this question.

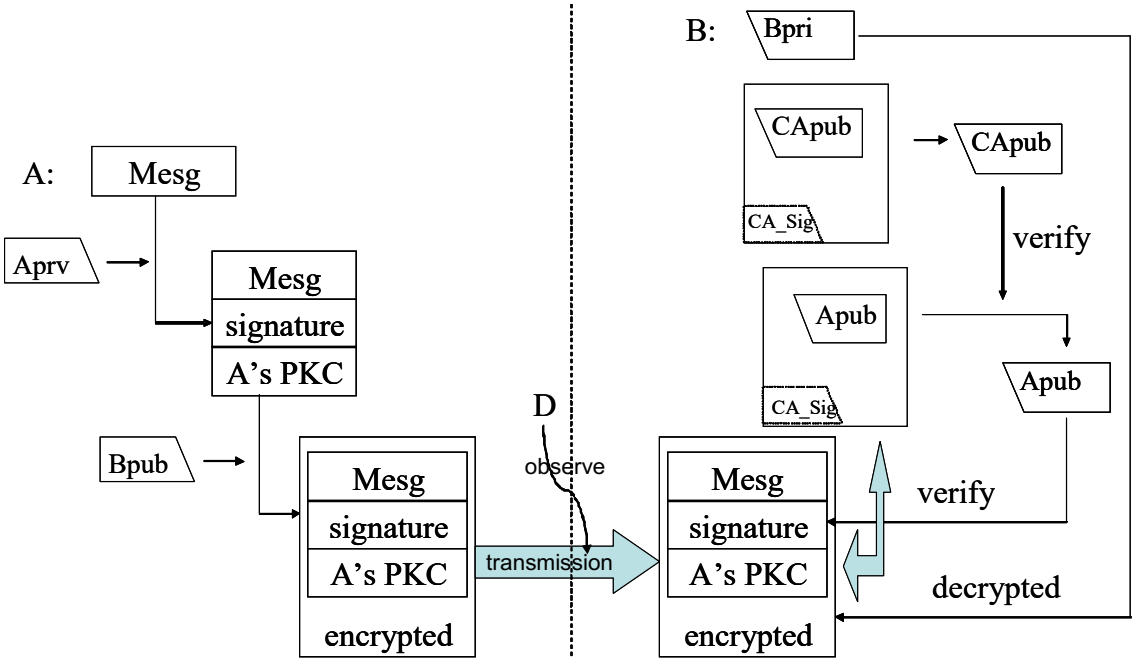
Q3. (15%)

(1) (5%) Alice uses RSA public key encryption system and her public key is $(e_A, n_A) = (23, 77)$, what is Alice's private key (d_A, n_A)?

(2) (10%) If Bob's public key is $(e_B, n_B) = (5, 91)$ and private key is $(d_B, n_B) = (29, 91)$, 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.

Q4. (20%)

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



(a) (5%) Suppose A sent a message to B yesterday. Today, he denies that he had sent the message before. How can B show evidence to a third party that A had really sent the message before?

(b) (5%) 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?

(c) (10%) 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?

Q5. (10%)

The Diffie-Hellman (DH) key agreement scheme supports 2 parties to exchange a secret session key for communication. Describe how to extend the DH key agreement scheme to support 3 parties to exchange a secret session key (sk). Prove your result.

Q6. (15%)

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:

I. A sends Aprv(Bpub(M)) to B
II. A sends Aprv(H(M)), Bpub(M) to B
III. A sends Aprv(H(M)), Bpub(H(M)) to B
IV. A sends Aprv(H(M)), Bpub(K), Ek(M) to B

(a) (5%) Which of the above approach is wrong? Explain your answer.
(b) (10%) 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.

Q7. (10%)

Given a modular exponentiation algorithm for n-bit integers that needs about n^3 operations, how much does performance deteriorate by moving from 1024-bit to 2048-bit RSA?

In your answers, you should show the detailed steps of your solution instead of listing the answer only.

No late submission is allowed.

Program with running error will not get mark.