Assignment 2: COMP90043
Due Date: 9 AM September 18, 2017
Assignment is worth 7.5% of the total marks

1. Submit the answers to Part A. You should also work out a solution to Part B, which will not be marked.
2. A Discussion forum thread Assignment 2 has been created on LMS. Any clarification offered on this forum will be considered as a part of the specification of the Assignment.
3. The assignment contributes to 7.5% of the total.
4. Answers must be submitted as a PDF file via the comp90043 Assignment 2 Turnitin submission form on LMS by the due date. Late submissions will attract a penalty of 10% per day (or part thereof). Please ensure your name and login name are presented.
5. **I suggest all of you to enroll "Academic Integrity Module" on your LMS home and take the Quiz in the module. You will be submitting your work on Turnitin, so do not share your answers with others. You are welcome to discuss strategies to answer the questions, but not to share the work.**

Part A: Questions

1. (2.5 marks) This question is concerning properties of Textbook RSA cryptosystem.

    a. RSA in small parameters: Assume that Alice chooses two primes
    352190187210465190186 61 and 12532072192921
    to construct her RSA keys. Determine the smallest valid RSA public key and its corresponding private key for Alice. **Show the detailed workings with an explanation justifying your answer**. You can use magma calculator from http://magma.maths.usyd.edu.au/magma/ If you use algorithms such as EEA or magma, show the workings.

b. This question is about the multiplicative property of the textbook RSA algorithm.

We showed in the workshop that basic RSA is not secure for chosen ciphertext attack. The same idea can also be applied to create blind signatures. Assume that Alice's public keys are $[n, e]$ and her private key is d. Explain how Bob could create Alice's signature on a message of choice m using the concept of blinding. Note that that Bob will not have access to private key d, but can request Alice to sign a blinded message.

Your solution **should also show the workings of the above blinding procedure using a random RSA key for Alice**. Your answer here should include the following:

i. Your selection of two random primes, each of length at least 300 digits.
ii. the public key e be smallest valid public key.
iii. Determine the private key d.
iv. A random message m of length at least 400 digits.
v. A blinded message m_b.
vi. Signature of m through blinded process.
vii. Direct signature of m using the private key.

Note: the last two items should be identical. Any code written for the above should be included as an appendix.

c. Assume that Alice has chosen a large RSA modulus n such that factorization is impossible with reasonable time and resources. She also then chooses a large random public exponent $e < n$ for which the RSA problem is also not practical. However Bob decides to send a message to Alice by representing each alphabet character as an integer modulo 26 and then encrypting each number separately using Alice's public address n, e. Is this a secure method? If not describe the most efficient attack against this method. Also, suggest a countermeasure to this attack.

2. (2.5 marks) A question on HASH, MAC and signatures.

a. Now, consider the following hash function. Here, messages are represented as series of numbers from Z_n, integers modulo n: $M = \{a_1, a_2, \cdots a_t\}$ for some integer $t \geq 1$. The hash function is defined as follows:

$$h(M) = (\sum_{i=1}^{t}(a_i)) \ mod \ n,$$

where n is a number agreed in advance.

For each of the key requirements of hash function, viz. one-way property, second image resistance and collision resistance, state if the above hash function satisfy the requirement or not. **You need to explain your reasons for your answers.**

b Now, consider a variation of the hash function for the messages represented as sequences of integers modulo n. The function is defined as follows:

$$h(M) = (\sum_{i=1}^{t}(a_i)^2) \ mod \ n,$$

where n is a large number whose factorization is unknown. For each of the

For each of the key requirements of hash functions, one-way property, second image resistance and collision resistance, state if the above modified hash function satisfy the requirement or not. **You need to explain your reasons for your answers.**

c. Explain how Diffie-Hellman(DH) key agreement protocol is vulnerable to man-in-the-middle attack. Is it possible to secure DH key agreement protocol against this attack by using each of the following primitives? **If your answer is yes, sketch the method. If the answer is no, give reasons.**

i. Message Authentication Codes

ii. Public Key Digital Signatures.

iii. Hash functions.

3. (2.5 points) This question is about Protocols.
An alternative key distribution method suggested by a network vendor is illustrated in the figure below: (Fig. 14.18 of the textbook).

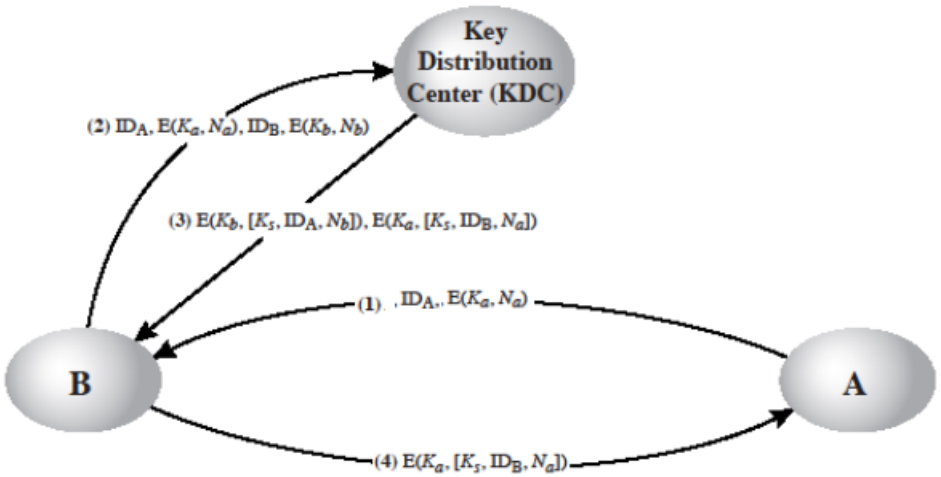

Figure 1: Fig. 14.18 of the Textbook

a. Describe the scheme.

b Compare this scheme to that of the scheme discussed in lectures (Fig 14.3 of the textbook-Given below).

c. Comment on the security of the new scheme.

d. What is the advantage of this scheme? Discuss the pros and cons.

e. Give an estimate of the memory requirements of KDC and the users with respect to storing key information.

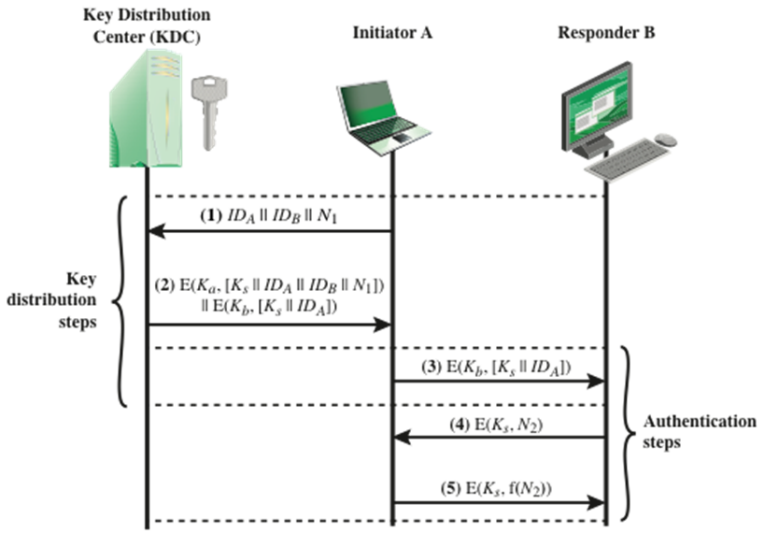

Figure 14.3 Key Distribution Scenario

Part B: Questions for Self Study (No need to submit answers for this part)

1. The textbook lists seven requirements of Hash functions. Out of these, one-way property, second image resistance and collision resistance are the three key requirements. Describe these three requirements.

2. What is the main difference between message authentication codes and digital signatures?

3. A variant of ElGamal cryptosystem over the prime field $GF(q)$ given as follows. Assume the parameters as given in the ElGamal.pdf. Let $y_A = a^{x_A} \mod q$, be the public address of Alice, where $x_A, 1 < x_A < q-1$, is Alice's private key. Encryption function is defined as follows:

$$E(M) = C_1, C_2,$$

where $C_1 = a^k \bmod q$, where k is a random integer $1 \leq k \leq q-1$, $C_2 = K \oplus M$, where $K = y_A^k \bmod q$ and $\oplus$ is binary exclusive or function applied to binary representation of K and M.

a. Describe the Decryption Function $D(C_1, C_2)$ that Alice can use to recover the message.

b. Show how the security of the encryption function is based on Computational Diffie-Hellman (CDH) problem.

CDH Problem: Let q be a prime number and a be a generator of the cyclic multiplicative group of modulo q. Given a^x, a^y, the CDH problem computes a^{xy}.