The University of Melbourne
School of Computing and Information Systems
COMP90043 Cryptography and Security

Assignment 2, Semester 2 2018

Due Date: September 17, 09:00AM

Objectives

To improve your understanding of the Euclid's algorithm, divisibility properties and classical ciphers. To develop problem-solving and design skills. To improve written communication skills.

Questions

1. [8 marks] Alice chooses two primes 484124774002102678821442007499625854054528 1 and 7120104115728581516059224292256265185280 01 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 need to attach any code you implemented in appendix, or mention the tools you used.

2. [20 marks] 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 $< n, d >$. Explain how Bob could create Alice's signature on a message of choice m using the concept of blinding. Note 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 should typically include the following:

   (a) Your selection of two random primes, each at least 10^{256}.

   (b) The public key e be smallest valid public key.

   (c) Determine the private key d.

   (d) A random message m which is at least 10^{500}.

   (e) A blinded message m_b.

   (f) Signature of m through blinded process.

   (g) Direct signature of m using the private key.

   Note: Any code written should be included in appendix. Any tools used to assist your calculation must be listed, and record commands you used (if there is any).

3. [12 marks] 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.**

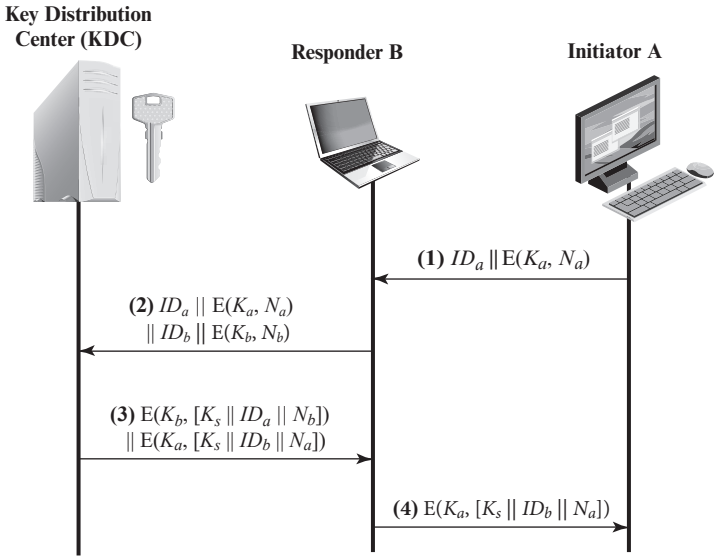
   (a) Message Authentication Codes

   (b) Public Key Digital Signatures.

   (c) Hash functions.

4. [8 marks] 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 key $< n, e >$. Is this method secure? If not, describe the most efficient attack against this method. Also, suggest a countermeasure to this attack.

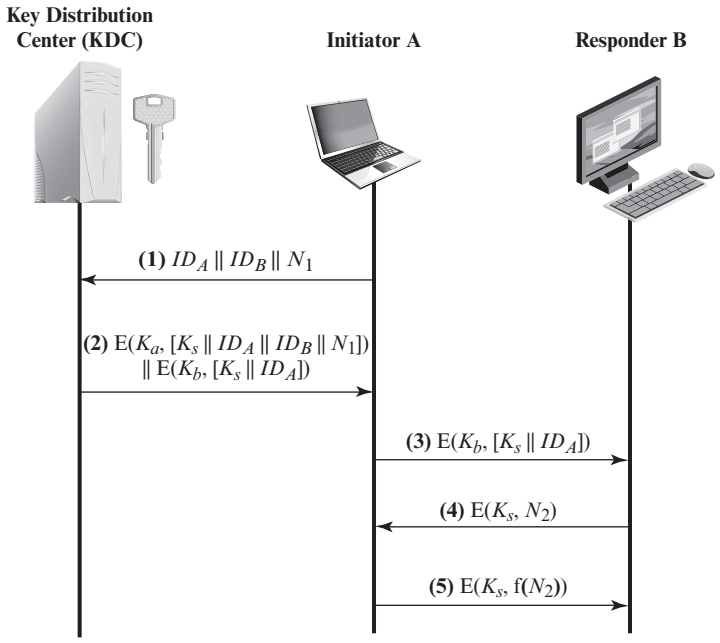
5. [15 marks] An alternative key distribution method suggested by a network vendor is illustrated in the figure below.



   (a) Describe the scheme in steps.

   (b) Give an estimation of the key storage requirements of both the KDC and users. You may need to make some appropriate assumptions.

   (c) Compare this scheme to the one discussed in the lecture (Fig 14.3 of the text-book - given below). You should focus on at least the following aspects: security, efficiency, authentication, whether a replay attack can be detected.



6. [12 marks] Suppose that any message can be represented as $M = \{a_1, a_2, \cdots a_t\}$ for any length of message $t \geq 1$. A variation of hash function has its output represented by a number from Z_n. The hash function is defined as:

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

where n is a large number whose factorization is unknown.

Does the above hash function satisfy the following requirements? Explain the reason for each of your answer. Give examples to support your justification if necessary.

(a) one-way property

(b) second preimage resistance

(c) collision resistance

Submission and Evaluation

- You must submit a PDF document via the COMP90043 Assignment 2 Turnitin submission form on LMS by the due date. Handwritten, scanned images, and/or Microsoft Word submissions are not acceptable — if you use Word, create a PDF version for submission.
- Late submission will be possible, but a late submission will attract a penalty of 10% per day (or part thereof).
- This assignment contributes 7.5% of the total marks in this subject. Marks are primarily allocated for correctness, but how clearly you communicate your thinking will also be taken into account.
- We expect your work to be neat — parts of your submission that are difficult to read or decipher will be deemed incorrect. Make sure that you have enough time towards the end of the assignment to present your solutions carefully. Time you put in early will usually turn out to be more productive than a last-minute effort.
- You are reminded that your submission for this assignment is to be your own individual work. For many students, discussions with friends will form a natural part of the undertaking of the assignment work. However, it is still an individual task. You are welcome to discuss strategies to answer the questions, but not to share the work (even draft solutions) on social media or discussion board. It is University policy that cheating by students in any form is not permitted, and that work submitted for assessment purposes must be the independent work of the student concerned.

  Please see `https://academicintegrity.unimelb.edu.au`

If you have any questions, you are welcome to post them on the LMS discussion board *so long as you do not reveal details about your own solutions.* You can also email the Head Tutor, Lianglu Pan (`lianglu.pan@unimelb.edu.au`) or the Lecturer, Udaya Parampalli (`udaya@unimelb.edu.au`). In your message, make sure you include COMP90043 in the subject header. In the body of your message, include a precise description of the problem.