The University of Melbourne

School of Computing and Information Systems

COMP90043: CRYPTOGRAPHY AND SECURITY

Mid Semester Test, Second Semester, 2021

Test Duration: 5 minutes Reading+ 40 minutes Actual Test + 30 minutes Uploading.

Instructions to Students:

- Total marks for the test is 50 (Worth 10% of the final mark in the subject).
- Note that the total time for writing is only 40 minutes.
- Test will be open on 5.15PM and you should stop writing by 6.0 PM. You will have 30 minutes for uploading. Hence you should complete the submission by 6.30PM Australian Eastern Standard Time (AEST). **A late submission will attract a penalty of 2.5 marks per minute late.**
- The test will have two parts: Part A is a quiz on canvas, Part B is this assignment and will have three questions.
- The test is open book, which means you may only use course materials provided via the LMS or the text book but must not use any other resource including the Internet.
- You also must not contact or communicate with any other person (other than teaching team) or make use of the Internet.
- Solutions must be written on blank A4 page paper with pen and pencil. You must write your solutions to each question on a new sheet of paper by clearly identifying the question number.
- You must not use tablet or any electronic device to generate your solution.
- Scanning instructions are already made available on Canvas in an announcement.

Declaration: By submitting this exam, you certify that you complied with "Declaration of Academic Honesty":

- The answers I am submitting for this assessment are my own unassisted work; and
- I have not made any use of communications devices or channels such as mobile phones, text messages, WeChat or WhatsApp, email, or other messaging technologies, while undertaking this assessment;
- I have not made use of any material outside of what is specified under Authorized Material of this assessment;
- I have not made use of any world-wide web or internet based resources, including google and other search services, Wikipedia, and StackOverflow;
- I have not taken any actions that would encourage, permit, or support other enrolled students to violate the Academic Honesty expectations that apply to this assessment.

Part A

Please complete the Quiz on Canvas available at *Assignments - Mid-Semester Test - Part A*

Part B: This Assignment:

1. Basic Numbers and CRT

   (a) [5 Marks] Find the smallest non-negative remainder of

   $(1271^{9897801} + 41)^{1342}$ divided by 101.

   Show your working.
   HINT: You may need to use various simplifying ideas discussed in lectures and workshop including Euler's and Fermat's theorems.

   (b) [5 Marks] Find a smallest non-negative number that satisfies the following:

   $$x \bmod 41 = 10$$
   $$x \bmod 51 = 33$$

   Show your workings by completing all steps on pen and paper.

2. RSA

   (a) [4 Marks] While cryptanalysing the RSA modulus 16637, an agent notices that

   $$8254^2 \bmod 16637 = 1.$$

   Show how the agent can use the above fact to factorize the modulus. Show your workings.

   (b) [6 Marks] Alice choses two primes p = 31 and q = 37 to compute her RSA keys. Determine the minimum possible encryption key e and then compute the corresponding decryption key d. As discussed in the subject, remember to present the keys in the form of $< n, e >$ and $< n, d >$.

3. The following equations and figure describe one of the standard modes of usage of symmetric key encryption.

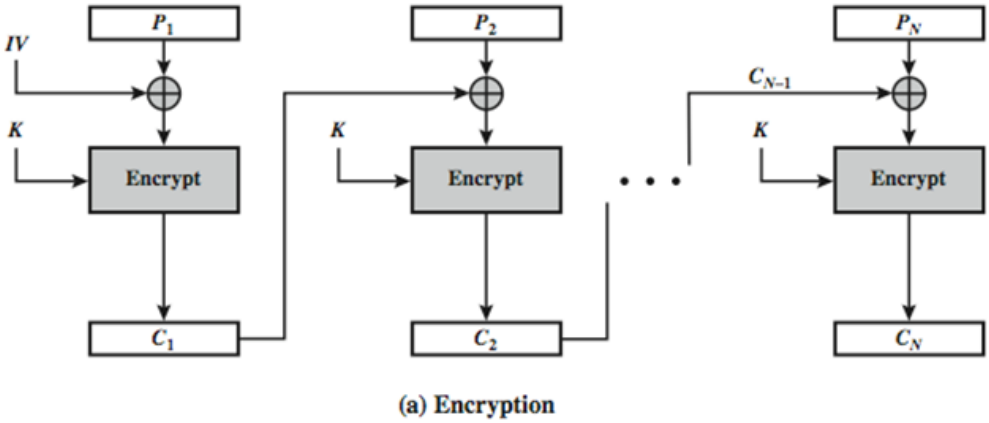

Figure 1: A Standard Mode of Encryption

Encryption:

$$C_1 = (E_K[IV \oplus P_1]).$$
$$C_j = (E_K[C_{j-1} \oplus P_j]), j > 1.$$

(a) [2 marks] What is the name of this mode?

(b) [2 Marks] Using the notations available in the above figure, complete the following decryption functions.
Decryption:

$P_1 =$ .....

$P_j =$ .....

(c) [2 marks] Can encryption of multiple blocks of a message be computed in parallel? Can decryption? Briefly explain your reasoning in each case.

(d) [2 Marks] What is the effect on the decrypted plaintext if a one-bit error occurred in the transmission of a ciphertext block C_j? How far does the error propagate?

(e) [2 marks] Describe a possible attack if the same IV is used to encrypt two messages.
HINT: consider that some of the blocks might be identical between two different messages

END OF EXAMINATION

