The University of Melbourne

Department of Computing and Information Systems

COMP90043-CRYPTOGRAPHY AND SECURITY

November, 2020

Exam Duration: 15 minutes reading + 120 minutes Exam writing + 30 minutes uploading

Authorised Materials: The exam is open book; You may only use course materials provided via the LMS or the text book but must not use any other resource including the Internet (See also next page). You can use any notes prepared by yourself. You may use calculators though calculators are not required to answer questions.

Instructions to Students:

- Total marks for the exam is 40 (Worth 40% of the final mark in the subject).
- Note that the total time to read, complete the work, scan and upload your responses to this test is 2 hours and 45 minutes. The last 30 minutes is for scanning and uploading your work. Usual exam rules apply. **Note that after 5:45 PM the exam may not be available.**
- Exam will be open on 3:00 PM and you must submit by 5:45 PM Australian Eastern Daylight Time (AEDT). A late submission will attract a penalty of 3 marks per minute late.
- The exam will have two parts: Part A is a quiz on canvas, Part B is this assignment which has 10 questions.
- 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.

continued on next page

- Scanning instructions are already made available on Canvas in an announcement.

- A discussion forum will be available during the exam for any exam content related issues.

- During the exam, for any non-content-related support, please contact: Inside Australia: 13 6352 / Outside Australia: +61 3 9035 5511 [select option 1, then select option 1 again].

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.

continued on next page

Part A

Please complete the Quiz on Canvas available at *Assignments - Semester 2 Exams, 2020 - Exam Part A*

Part B: This Assignment:

1. [2 marks] List two general methods employed to protect against replay attacks in protocols studied in the subject? What are the main relative advantages and disadvantages of these two methods?

2. [4 marks] For each of the following ciphers, compute number of possible non-trivial keys. A trivial key is the one which maps all elements to themselves.

   (a) $Cipher_1$: A Vegenere Cipher defined over the alphabet $\mathbf{GF}(29)$ having a key of length between m_1 and m_2 characters.

   (b) $Cipher_2$: A transposition cipher over the alphabet $\mathbf{GF}(29)$ with a key length m_3.

   (c) $Cipher_3$: A product cipher defined by product of $Cipher_1$ and $Cipher_2$, where the plaintext symbols first encrypted by $Cipher_1$ and then encrypted by $Cipher_2$.

3. [4 marks] Evaluate or simplify the following expressions. Show the steps in your calculations.

   (a) $a^{p-1} + (p-1)^a \bmod p$, where p is a prime number and a is an odd integer co-prime to p.

   (b) Solve x in $3x^{14} + 4x^{10} + 6x - 18 \equiv (0 \bmod 5)$.

4. [3 marks]

   (a) What are the important requirements of a modern symmetric cipher?

   (b) We studied Fiestel cipher which is an example of an iterated block cipher. We consider a version of Fiestel cipher with two rounds whose encryption ladder is illustrated below. Draw the corresponding decryption ladder. You may assume any missing information required in the function definitions and data formats.

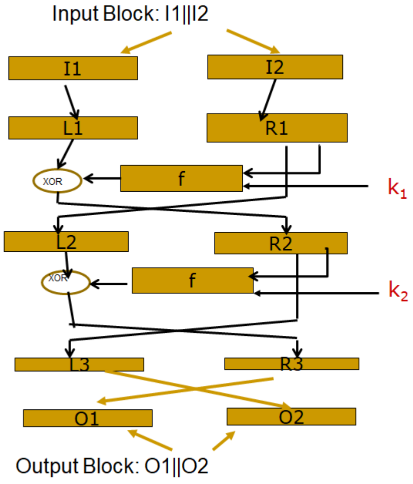

Figure 1. Encryption ladder of a two round Fiestel Cipher

continued on next page

5. [2 marks] In RSA algorithm, if two primes $p = 29$ and $q = 41$ are used, what are the three smallest possible values for d? Please show your working (however, you don't need to show the steps for calculating modulo inverse).

6. [3 marks] Consider $\mathbf{GF}(2^3) = \mathbf{GF}(2)[x]\ mod\ (x^3 + x^2 + 1)$, a field with 8 elements.

   (a) Express all the elements of $\mathbf{GF}(2^3) = \mathbf{GF}(2)[x]\ mod\ (x^3 + x^2 + 1)$ as polynomials.

i	Elements:x^i	As Polynomials
$-\infty$	0	
0	1	
1	x	
2	x^2	
3	x^3	
4	x^4	
5	x^5	
6	x^6	
7	x^7	

Table 1: Elements of $GF(2^3)$ as powers of x

   (b) Find the multiplicative inverse of the polynomial $x^2 + x$ in the above field.

7. [4 marks] This question is about hash and MAC.

   (a) Consider the following hash function based on RSA. The key $< n, e >$ is known to the public. A message M is represented by blocks of predefined fixed size $M_1, M_2, M_3, ..., M_m$, $m \geq 1$ such that $M_i < n$ and positive for all $i \leq m$. The hash is constructed as follows: take the first block, XOR with the second block, take the result and XOR with the third block, etc. Encrypt the final result using RSA. For example, the hash value of a message consisting of m blocks is calculated by

continued on next page

$$H(M) = H(M_1, M_2, ..., M_m) =$$
$$(M_1\ XOR\ M_2\ XOR\ ...\ XOR\ M_m)^e \bmod n$$

Does this hash function satisfy each of the following requirements? Justify your answers (with examples if necessary).

i. Variable input size
ii. Fixed output size
iii. Efficiency
iv. Preimage resistant
v. Second preimage resistant
vi. Collision resistant

(b) What are the consequences of the above hash function being used in a public key signature algorithm?

8. [3 mark] Assume the textbook RSA signature which uses no hash for this question. Marvin (an adversary) accidentally discovers a series of message and signature pairs in Alice's computer.

$$(m_1, s_1), (m_2, s_2), (m_3, s_3), (m_4, s_4) \text{ and } (m_5, s_5),$$

where $s_i = (m_i)^d\ mod\ n, 1 \leq i \leq 5$.

Marvin wishes to create some new messages that are the functions of the above discovered messages as follows:

Index	New message	Function
1	$f_1 =$	$m_3\ m_4^3 + m_5$
2	$f_2 =$	$m_1^3\ m_2^4\ m_4^{573}$
3	$f_3 =$	$m_1 + 19897\ m_3 + 23987\ m_5$

Which of the above messages could he forge and which could he not? Explain both the reasoning and the construction steps involved in the forged signatures.

9. [2 marks] The following key distribution scenario was discussed in the subject, which is based on Needam/Schroder protocol where each user shares a unique master key with the key distribution centre (KDC).

Is this protocol susceptible to Man-in-the-Middle attack? If Yes, explain how it is susceptible. If No, explain why the attack is not effective. You can assume the symmetric key algorithm used is strong.

continued on next page

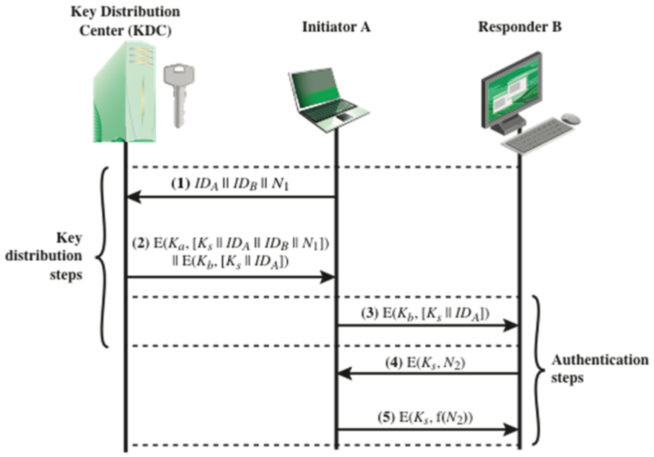
Key Distribution Center (KDC)
Initiator A
Responder B
(1) $ID_A \| ID_B \| N_1$
Key distribution steps
(2) $E(K_a, [K_s \| ID_A \| ID_B \| N_1]) \| E(K_b, [K_s \| ID_A])$
(3) $E(K_b, [K_s \| ID_A])$
(4) $E(K_s, N_2)$
Authentication steps
(5) $E(K_s, f(N_2))$

Figure 14.3 Key Distribution Scenario

10. [3 marks] For this question, we use the key distribution scenario in the question above with only one difference that the encryption function is replaced by a version of a one-time-pad encryption where the encryption E is bitwise XOR of the key and message. For example, in Step 3,

$$E(K_b, [K_s||IDA] = K_b \oplus [K_s||IDA].$$

You can assume that both master keys and session keys are sufficiently long as required by the one-time-pad function.

What are the consequences of this modification to the protocol? Explain your answer.

END OF EXAMINATION