The University of Melbourne

Department of Computing and Information Systems

COMP90043 CRYPTOGRAPHY AND SECURITY

Practice Exam 2020

Exam Duration: 15 minutes reading + 120 minutes writing + 30 minutes scanning and uploading;

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 uploading your work. Usual exam rules apply.
- The exam will have two parts: Part A is a quiz on canvas, Part B is this assignment and will have 10 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.

continued on next page

Part A

Please complete this part on Canvas at *Assignments - Practice Exam - Part A*

1. (2 marks) This question contains several multiple choice questions. For each question, pick exactly one of the choices.

   (a) The science of breaking ciphers is called ________________.

      i. Cryptography
      ii. Cryptology
      iii. Cryptanalysis
      iv. Decryption

   (b) CVE stands for ________________.

      i. Common Vulnerability Exposure
      ii. Critical Vulnerability Evaluation
      iii. Critical Vulnerability Exposure
      iv. None of the above

   (c) If a and b are the secrets used by Alice and Bob respectively in Diffie-Hellman key exchange protocol, the common secret shared by Alice and Bob at the end of the protocol is ________________.

      i. $a \cdot b$
      ii. a^b
      iii. b^a
      iv. None of the above

   (d) What is the use of Encryption?

      i. Integrity.
      ii. Non-repudiation.
      iii. Confidentiality.
      iv. All of the above.

2. (8 marks) Fill in the blanks.

   (a) $(18 + 23) \bmod 26 =$ ________________.
   (b) $22^{-1} \bmod 23 =$ ________________.
   (c) $x^{101} \bmod\ 101 =$ ________________.
   (d) p is a prime, $x \neq 0$, $x^{p-1} \bmod p =$ ________________.
   (e) $\varphi(p) =$ ________________,
   where p is a prime and φ is the Euler's function.
   (f) $2^{144}3^{132}5^{100} \bmod 4 =$ ________________.
   (g) If m is a positive even integer, $(1 + 2 + 3 + 4 + ... + m) \bmod (m + 1) =$ ________________.
   (h) Let $m \geq 1$, $(1 + 2 + 4 + 8 + ... + 2^{m-1}) \bmod (2^m) =$ ________________.

continued on next page

Part B: This Assignment:

3. Classical Ciphers (3 marks)

   (a) The Vatsyana cipher is a specific version of a classical substitution cipher with the following two conditions:

      i. A character x is mapped to another distinct character y and

      ii. If a character x is mapped to y, then the character y will be mapped to x. In other words, substitution happens in pairs where the characters in each pair are mapped to each other.

   How many possible mappings (keys) are there when the cipher is defined over 26 English characters? Briefly justify your answer.

   (b) Consider the following version of a classical cipher where plain text and cipher text elements are integers from 0 to 25. The encryption function, which takes any plain text p to a cipher text c, is given by

$$c = E_{a,b}(p) = (ap + b) \ mod \ 26,$$

   where a and b are integers less than 26.

   Show how an adversary can attack the system under the "Chosen Plaintext Attack" model.

4. (3 marks) This question is about computing the inverse of a number modulo n, where n a positive integer. Note: Inverse of a number a mod n is a number x such that $xa = 1 \bmod n$. In this semester, we studied methods for finding inverse modulo n using the Extended GCD algorithm ($XGCD$) and Fermat's or Euler's theorems.

   (a) When n is a prime number, write a pseudocode for the function Inverse(a, n) which finds the inverse of a modulo n using the properties of the Fermat's theorem.

   (b) The Extended GCD algorithm ($XGCD$), also known as the Euclidean algorithm, takes two integers a and b as inputs and returns three integers g, x and y such that

$$a\ x + b\ y = g,$$

   where g is the greatest common divisor of the input integers.

   You have provided the results from the XGCD function and exponentiation modular identities below:

      i. $XGCD(12986, 46799) = 1, 8905, -2471$

      ii. $XGCD(12, 39) = 3, -3, 1$

      iii. $XGCD(17, 29) = 1, 12, -7$

      iv. $12^{29} \bmod 31 = 13$

      v. $10^{29} \bmod 31 = 28$

   Now determine the following numbers:

      i. $12^{-1} \bmod 39$

continued on next page

ii. $12986^{-1} \bmod 46799$

iii. $17^{-1} \bmod 29$

iv. $12^{-1} \bmod 17$

v. $12^{-1} \bmod 31$

vi. $10^{-1} \bmod 31$

5. (4 marks) This question is about hash and MAC.

(a) What is the main difference between hash functions and message authentication codes (MAC)?

(b) Consider a version of the practical RSA signature algorithm discussed in the lectures. Let n, e be Alice's RSA public key and d be Alice's private key. The signature of a message $m, 0 < m < n - 1$ is given by

$$(m, s = (h(m))^d \bmod n),$$

where h is a hash function. Answer the following questions:

i. What is the verification equation for this hash function?

ii. A researcher discovers that the hash function used in the above scheme failed the second preimage resistance property. What are the consequences for the collision resistance property of the function and the security of the signature algorithm? Explain your answers.

(c) In the subject, we looked at a few requirements of Hash functions. Out of those, one-way property, second image resistance and collision resistance are the three key requirements. Describe these three requirements.

6. (2 marks) Consider the finite field $GF(2^3)$ as poynomails modulo $1 + x^2 + x^3$.

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

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

(a) Complete the polynomial representations of the missing elements (marked as ①, ②, ③ and ④) of the table.

(b) Solve the equation in y: $xy = x^3$.

(c) Compute $x^3 + x^6 + x^5$.

continued on next page

7. (3 marks) Consider the ElGamal signature scheme over the prime field $GF(q)$ given in lectures. Let H be a public hash function, $y_A = a^{x_A} \bmod q$ be the public key of Alice, where $x_A, 1 < x_A < q-1$ is the private key and a is a primitive element in the field. Alice uses the following equation to define the ElGamal signature scheme:

$$k\ S_2 + x_A S_1 = m \bmod (q-1),$$

where $m = H(M)$, M an arbitrary message and k, S_1 and S_2 are the signature parameters used in the scheme.

   (a) What are the signing and verification equations?

   (b) What is the consequence of using same k for signing two different messages?

   (c) What is the consequence if the function H used in the signing equation violates the second preimage resistant property of hash functions?

8. (3 mark) Assume the RSA signature parameters for this question. Marvin (an adversary) accidentally discovers the following message and signature pairs in Alice's computer.

$$(m_1, s_1) \text{ and } (m_2, s_2),$$

where $s_1 = (m_1)^d\ mod\ n$ and $s_2 = (m_2)^d\ mod\ n$. To his amazement, he discovers that the message he wanted to forge was exactly $m = (m_1^3\ m_2)\ mod\ n$. Is it possible to forge Alice's signature on the message m? If so, describe how to construct a forged signature on the message. Note that in this question we assume the basic textbook RSA signature scheme which do not employ any hash function.

9. (3 marks) Alice and Bob exchange their authentic RSA key parameters. Let n_a, e_a and n_b, e_b be public RSA parameters of Alice and Bob respectively. Similarly let d_a and d_b be private RSA keys of Alice and Bob respectively. Let $E_k()$ and $D_k()$ be encryption and decryption functions of the popular symmetric key cipher AES. Bob wants to send a large file *FILE* to Alice as explained below:

   (a) Chooses a random session key k_s, and encrypts as $C = k_s^{e_a} \bmod n_a$.

   (b) Encrypts *FILE* using the AES cipher as: $ENC\_FILE = E_{k_s}(FILE)$.

   (c) Computes $h = \text{HASH}(FILE)$, where HASH is a public hash function.

   (d) Computes the signature as $S = h^{d_b} \bmod n_b$.

   (e) Sends (ENC_FILE, C, S) to Alice.

   Now complete the missing parameters in the following steps to be performed by Alice if the messages are error free and not tampered.

   (a) $k_s =$ ________________ modn_a.

   (b) $FILE\_RECEIVED =$ ________________

   (c) $\hat{h} = \text{HASH}($ ________________ $)$.

   (d) $S^{e_b} \bmod n_b =$ ________________

continued on next page

10. (2 marks) The following equations and figure describe one of the standard modes of usage of symmetric key encryption.

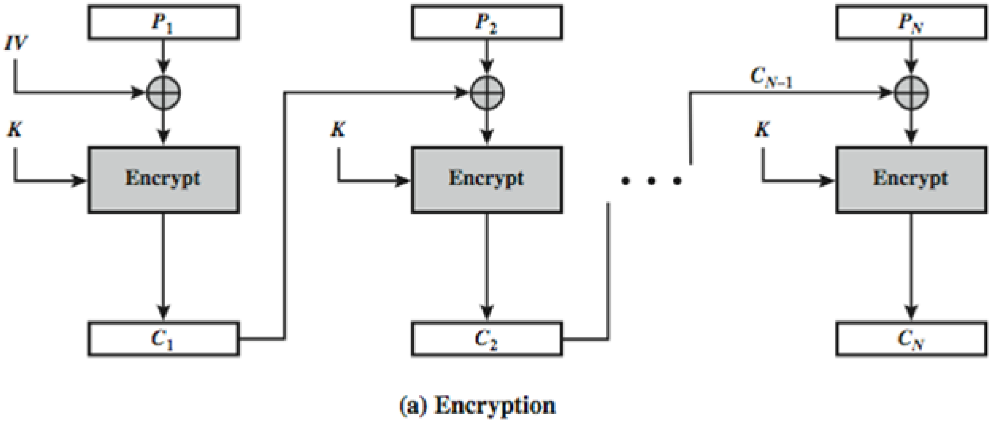

Figure 1: A Standard Mode of Encryption

Encryption:

$$C_1 = (E_K[IV \oplus P_1]).$$

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

(a) What is the name of this mode?

(b) Expand the abbreviations and functions used in the equations:

i. IV

ii. K

iii. C_j

iv. P_j

v. $E_y[x]$

(c) Complete the equations for decrypting:

i. P_1.

ii. P_j.

11. (3 marks) Consider the following two protocols considered in the subject which are variations of Needham-Schroeder protocol:

Protocol A (Denning's Protocol):
1. A → KDC: $ID_A \mid\mid ID_B$
2. KDC → A: $E(K_A, [K_s || ID_B || T || E(K_b, [K_s || ID_A || T])])$
3. A → B: $E(K_B, [K_s || ID_A || T])$
4. B →A: $E(K_s, N_1)$
5. A → B $E(K_s, f(N_1))$

continued on next page

Protocol B (An improvement to Denning's Protocol):

1. A → B: $ID_A \mid\mid N_a$
2. B → KDC: $ID_B||N_b||E(K_b, [ID_A||N_A||T_b])$
3. KDC → A: $E(K_A, [ID_B, N_a||K_s||T_b])||E(K_B, [ID_A, K_s||T_b])||N_b$
4. A →B: $E(K_b, [ID_A||K_s||T_b])||E(K_s, N_b)$

(a) What is the role of T in Protocol A?

(b) What is Suppress-Replay Attack?

(c) Protocol A is susceptible to Suppress-Replay Attack. Explain why and suggest a remedy.

(d) Explain how Protocol B address the above susceptibility.

12. (4 marks)

(a) Describe the Diffie-Hellman (DH) key agreement protocol defined over the group of integers modulo p, where p is a prime number. You are welcome to use any assumptions required to complete the statement of the protocol. Your answer should include the public parameters of the scheme and series of messages exchanged between the users A and B.

(b) Show how this protocol is susceptible to a man-in-the-middle attack.

(c) Modify the protocol in part (a) so that it is secure against the vulnerability found in part (b) using the public key certificate scheme as defined in this subject. Briefly justify your solution. For your benefit, some relevant details about the certificate scheme are given below. You may have to fill in missing details if required.

- Let $[PU_{auth}, PR_{auth}]$ be the public and private key pair of the certificate authority.
- Let $E(PU, .)$ and $D(PR, .)$ be the public key encryption and decryption functions used in the scheme.
- The format of the certificate for a user A is given as $C_A = E(PR_{auth}, [T \parallel ID_A \parallel PU_A])$, where T is a timestamp.

END OF EXAMINATION