Student Number

The University of Melbourne

Department of Computing and Information Systems

COMP90043-CRYPTOGRAPHY AND SECURITY

Practice Exam 2019

Exam Duration: 120 minutes.

Reading Time: 15 minutes.

Length: This paper has 9 pages including this cover page.

Authorised Materials: None.

Instructions to Students: Print your student number at the writing box given at the top of this page. Answer all questions in this exam booklet. Total marks for the exam is 50. This exam is worth 40% of the final mark in the subject;

Calculators: No Calculators are permitted.

Library: This paper must be returned and not taken out of the exam hall.

For Marking only: The following table will be used to record the marks. Do not write anything in the table below.

1	2	3	4	5	6

1. (2 marks) This question contains several multiple choice questions. For each question, circle 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) (1 mark) What is the use of Encryption?
       i. Integrity.
       ii. Non-repudiation.
       iii. Confidentiality.
       iv. All of the above.

2. (2 marks) Are the following statements true or false? Indicate your choice by printing "TRUE" or "FALSE" next to the statements.

   (a) The OSI security architecture provides a systematic framework for defining security attacks, mechanisms, and services.

   (b) Finite fields of size p can be defined using arithmetic mod p, where p is a prime number.

   (c) The number 37 is prime so therefore all of the positive integers from 1 to 36 are relatively prime to 37.

   (d) Timing attacks are ciphertext attacks that are only applicable to RSA.

3. (10 marks) Fill in the blanks.

   (a) $x^{p-1} \bmod p, x \neq 0, p$ is a prime $= $ —————.

   (b) $x^{101} \bmod 101, = $ —————.

   (c) $\phi(p) = $ —————,
       where p is a primes and ϕ is the Euler's function.

   (d) Let $m \geq 1$, $(1 + 2 + 3 + 4 + ... + m) \bmod (m + 1), = $ ————-

   (e) $(18 + 23) \bmod 26 = $ —————,

   (f) $22^{-1} \bmod 23$.

   (g) $2^{144} 3^{132} 5^{100} \bmod 4 = $ ————-.

   (h) Let $m \geq 1$, $(1 + 2 + 4 + 8 + ... + 2^{m-1}) \bmod (2^m) = $ ————-

   (i) In the context of network security, ———— is the ability to limit and control
       the access to host systems and applications via communications links.

   (j) ————- prevents either sender or receiver from denying a transmitted mes-
       sage. Thus, when a message is sent, the receiver can prove that the alleged
       sender in fact sent the message and when a message is received, the sender can
       prove that the alleged receiver in fact received the message.

4. (5 marks)

   (a) What are the two important requirements of symmetric encryption as discussed
       in textbook?

   (b) Explain the workings of the classical substitution cipher.

(c) How many possible keys exist in a classical substitution cipher?

(d) What is a replay attack? Give an example of a reply attack and its counter measure.

5. (3 marks)

(a) Explain why CRC checksum used in network protocols cannot be used as a cryptographic hash function.

(b) What are the five basic requirements for cryptographic hash functions?

(c) Explain the birthday attack for hash functions. What does this attack imply for the security of hash functions?

6. (3 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		$[\qquad]$
4	x^4		$[\qquad]$
5	x^5		$[\qquad]$
6	x^6		$[\qquad]$
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 of the table.

(b) Compute $x^3 + x^6 + x^5$;

(c) Solve for t and w in the following simultaneous equations over the field.

$$x^2\, t + x^4 w = 1;$$

$$t + w = 1;$$

7. (4 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 $xa = 1$ mod n.

   (a) The Extended GCD algorithm ($XGCD$), also known as the Euclidean algorithm, takes two given 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.
   Write a pseudocode for the function **inverse modulo** n using the XGCD function given above. NOTE: There is no need for you write XGCD function.

   (b) You have been given the results from the XGCD function below:
      i. $XGCD(11137, 56799) = 1, 18916, -3709$

      ii. $XGCD(22, 67) = 1, -3, 1$

      iii. $XGCD(23, 37) = 1, -8, 5$

      Now determine the inverse of the following numbers:

      i. 22 mod 67

      ii. 11137 mod 56799

      iii. 23 mod 37

      iv. 37 mod 23

8. (4 marks) Consider the ElGamal crypto system over the prime field $GF(q)$ given in lectures. Let $y_A = a^{x_A} \bmod q$ 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.

   (a) Define ElGamal encryption and decryption functions.

   (b) State the hard problems on which the scheme is based.

9. (4 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) $k_s = \dots\dots\dots\dots\dots\dots \bmod n_a$.

   (b) $FILE\_RECEIVED = \dots\dots\dots\dots\dots\dots$

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

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

continued on next page

10. (4 marks) The following equations and figure describe one of the standard modes of usage of symmetric key encryption.
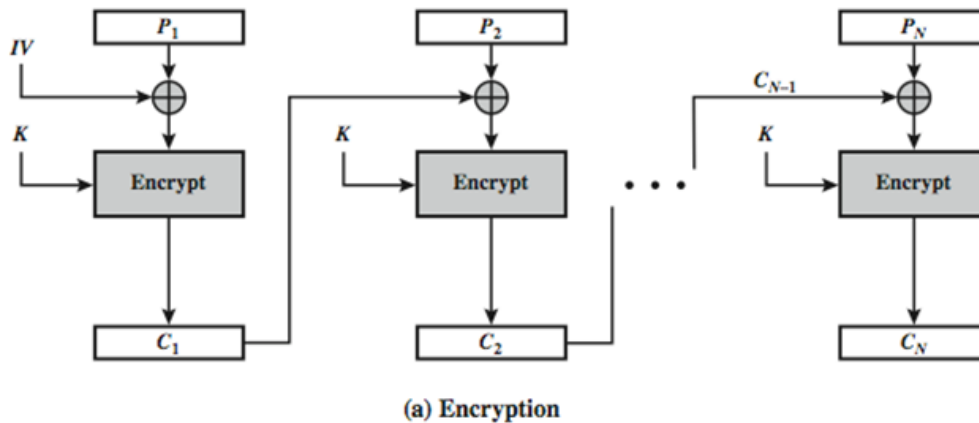

(a) Encryption

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 decryption below:

Decryption:
$P_1 = $ ———————.
$P_j = $ ———————.

(d) What is the effect on the plain text of a one bit error in the transmission of an encrypted "block C_j"?

11. (4 marks)

    (a) List four general categories of schemes for the distribution of public keys. Briefly explain one of the schemes.

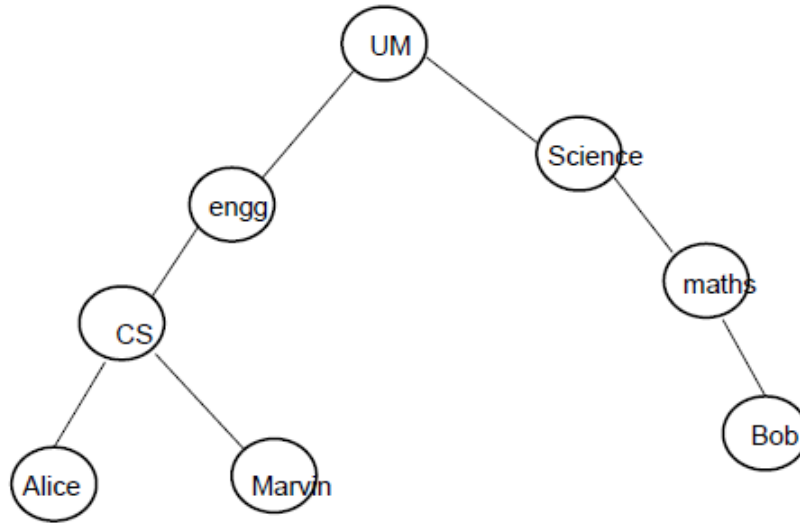   (b) Consider the hierarchy of Certificate Authorities (CAs) as in Figure 2. Show

Figure 2: A Hierarchy of Certificate Authorities.

an example of certificates used to navigate the hierarchy. What is the chain of certificates that user Alice needs to obtain in order to establish a certificate path to Bob? You can use X.509 conventions for the certificate chain discussed in the book, for example the certificate for Alice by the CA CS is represented as CS <Alice>.

12. (5 marks) This question is about hash and MAC.

    (a) What are the standard requirements of a cryptographic hash function?

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

    (c) Assume that Alice and Bob share a common key k. Then consider the following protocol:

        1. Alice computes $\text{MAC}_k(M_s) = m_a$ on the message M_s
        2. Alice $\rightarrow$ BoB : $< M_s \parallel m_a >$
        3. Bob receives $< M_r \parallel m_a >$
        4. Bob computes $\text{MAC}_k(M_r)$ and verifies if $m_a = \text{MAC}_k(M_r)$ holds.
        5. Accepts M_r if 4 holds, else rejects.

    Rewrite the above protocol using only a standard cryptographic hash function. Note: In the above protocol, $a \parallel b$ represents concatenation of a and b.

                    continued on next page

(d) (3 marks) In RSA, it is a normal practice to sign a $h(M)$, where h is an appropriate hash function instead of signing the message M directly. Explain why this is necessary.

END OF EXAMINATION