Student Number SOLUTION

The University of Melbourne

Department of Computing and Information Systems

CRYPTOGRAPHY AND SECURITY

September, 2018

Quiz Duration: 60 minutes + 5 minutes Reading Time.

Length: This paper has 10 pages including this cover page.

Authorised Materials: None.

Instructions to Students: Answer all questions in this exam booklet. Marks are indicated for each question, all subquestions receive equal weightage unless otherwise specifically mentioned.
Total marks for the test is 50. This is worth 10% of the final mark in the subject;

Exam Rules: You need to bring student card with you to the test. When instructed, please take seats in an orderly manner leaving one empty seat vacant between occupied seats. Do not open the paper until the reading time starts. Do not write during the reading time. When asked to write your response start with printing your student number on the first page. During the test, tutors will look for your student cards.

Calculators: No Calculators are permitted.

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

1	2	3	4	5	6	7

continued on next page

This page is a blank page

continued on next page

1. (10 marks) This question contains several multiple choice questions. For each question, circle at most one of the choices.

   (a) The three concepts that form what is often referred to as the CIA triad are ..... These three concepts embody the fundamental security objectives for both data and for information and computing services.

   i. confidentiality, integrity and availability
   ii. communication, integrity and authentication
   iii. confidentiality, integrity and access control
   iv. communication, information and authenticity

   (b) An original intelligible message fed into the algorithm as input is known as ....., while the coded message produced as output is called the .....

   i. decryption, encryption
   ii. plaintext, ciphertext
   iii. deciphering, enciphering
   iv. cipher, plaintext

   (c) A ..... attack involves trying every possible key until an intelligible translation of the ciphertext is obtained.

   i. brute-force
   ii. Caesar
   iii. ciphertext only
   iv. chosen plaintext

   (d) A common technique for masking contents of messages or other information traffic so that opponents are not able to extract the information from the message is..... .

   i. integrity
   ii. encryption
   iii. analysis
   iv. masquerade

continued on next page

(e) ..... attacks exploit the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

i. Brute-force
ii. Cryptanalytic
iii. Block cipher
iv. Transposition

(f) The ..... and ..... block cipher modes of operation are used for authentication.

i. OFB, CTR
ii. ECB, CBC
iii. CFB, OFB
iv. CBC, CFB

(g) Asymmetric encryption is also known as ..... .

i. public-key encryption
ii. private-key encryption
iii. optimal encryption
iv. digital-key encryption

(h) The effort required for a collision resistant attack is explained by a mathematical result referred to as the ..... .

i. Whirlpool
ii. birthday paradox
iii. hash value
iv. message authentication code

(i) The cryptographic hash function requirement that guarantees that it is impossible to find an alternative message with the same hash value as a given message and prevents forgery when an encrypted hash code is used is the..... .

i. collision resistance
ii. pseudorandomness
iii. preimage resistance
iv. second preimage resistance

continued on next page

(j) In symmetric key cryptography,

i. the same key is used for both encryption and decryption functions.

ii. the participants of the scheme must share the algorithms and the key.

iii. confidentiality and authentication cannot be simultaneously achieved between the sender and receiver.

iv. both (i) and (ii) apply.

2. (8 marks) Short Answer Questions (Please answer in the space provided).

(a) Let p be a prime number. Then for any positive $x < p$, $x^{p-1} \mod p =$ .....1.....

(b) $-1298 \mod 12 =$ .....10.....

(c) Given that $1653 = 3 \times 19 \times 29$, calculate: $\phi(1653) =$ .....1008....., ϕ is the Euler's function.

(d) $19^{-1} \mod 20 =$ .....19.....

(e) $9^{30}6^{2600}5^{33} \mod 7 =$ .....6.....

(f) $2^{144}3^{132}5^{100} \mod 100 =$ .....0.....

(g) For any positive integer k, $\phi(p^k) =$ .....$p^{k-1}(p-1)$..... where p is a prime number and ϕ is Euler's function.

(h) The minimum positive integer x that satisfies the following relations is .....24.....
$x = 3 \mod 7$;
$x = 4 \mod 5$.

continued on next page

3. (5 marks) Basic Numbers and Classical Symmetric systems.

   (a) (1 mark) As discussed in lectures and the textbook, what are the two requirements of symmetric encryption?

   - Strong Algorithm
   - A secret key shared by both sender & receiver

   (b) (1 mark) Consider the following version of a classical cipher where plain text and cipher text elements are from 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. Write down the decryption function for the above cipher:

   $p = (c - b)a^{-1} \ mod \ 26$

   (c) (3 marks) Let p be an odd prime number. For any positive $x < p$ and $x \neq 1$, show that

   $$x^{p-2} + x^{p-3}, \cdots + x + 1 \bmod p = 0.$$

   $1 + x + x^2 + \cdots + x^{p-2} \ mod \ p$

   $= \frac{1(1 - x^{p-1})}{1 - x} \ mod \ p$

   $= \frac{x^{p-1} - 1}{x - 1} \ mod \ p$

   $= (x-1)^{-1}(x^{p-1} - 1) \ mod \ p$

   $x^{p-1} \ mod \ p = 1$ (Fermat's Theorem)

   $= (x-1)^{-1}(1 - 1) \ mod \ p$

   $= 0$

4. (4 mark) Alice wants to setup her RSA keys (Textbook version) for signature. She chooses two large random primes p and q and the private exponent d. Fill in the blanks in the following which will help her to compute the standard RSA signature parameters.

   (a) Alice's RSA modulus n is ..... $p \cdot q$ .....

   (b) The public exponent e is found such that ..... $e = d^{-1} \ mod \ \varphi(n)$ .....

   (c) The signature for the message m is [..... m ....., ... m^d ..... mod ..... n .....].

   (d) The verification equation is ..... $(m^d)^e \ mod \ n == m$ .....

   S

continued on next page

5. (8 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 $xa = 1 \bmod n$.

   (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.

```
function inverse(a, n)
    g, x, y = XGCD(a, n)
    if g == 1 then
        return x % n
    else
        return "No inverse"
```

   (b) You have been given the results from the XGCD function below:

   i. $XGCD(23457, 78539912) = 1, 1670777, -499$

   ii. $XGCD(13, 29) = 1, 9, -4$

   iii. $XGCD(12, 21) = 3, 2, -1$

   Now determine the inverse of the following numbers:

   i. 23457 mod 78539912 — 1670777

   ii. 13 mod 29 — 9

   iii. 3 mod 13 — 9

   iv. 12 mod 21 — N/a

continued on next page

6. (10 marks) For the prime numbers $p = 29$ and $q = 31$, calculate the non-trivial RSA keys e and d, $e > 1$, satisfying the condition that d has the smallest possible values. Show detailed steps.

$n = p \cdot q = 29 \times 31 = 899$

$\varphi(n) = (p-1)(q-1) = 28 \times 30 = 840 = 2^3 \times 3 \times 5 \times 7$

$d = 11$

$840 = 11 \times 76 + 4$

$11 = 4 \times 2 + 3$

$4 = 3 \times 1 + 1$

$1 = 4 - 3 \times 1$

$1 = 4 - (11 - 4 \times 2) \times 1 = 4 \times 3 - 11$

$1 = (840 - 11 \times 76) \times 3 - 11 = 840 \times 3 - 11 \times 229$

$e = -229 \bmod 840 = 611$

continued on next page

7. (5 marks) The following equations and figure describe one of the standard modes of usage of symmetric key encryption.

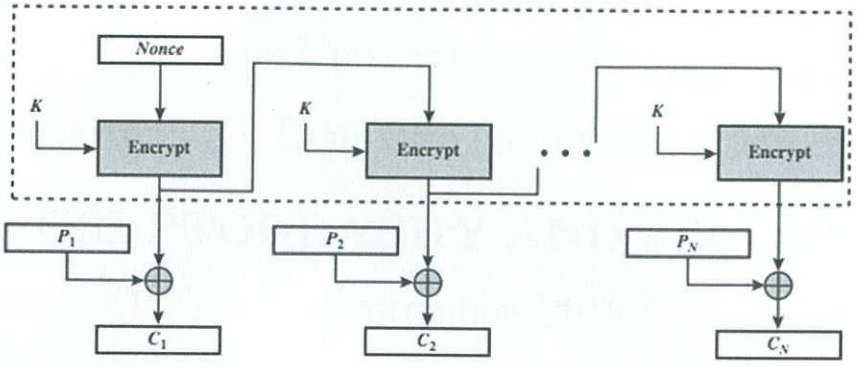

Figure 1: A Standard Mode of Encryption

Encryption: Let IV is the Initial Vector obtained from the Nonce generator.

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

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

(a) (1 mark) What is the name of this mode?

OFB (Output Feedback)

(b) (2 marks) Complete the equations for decryption below:

Decryption:

$P_1 =$ $C_1 \oplus E_K[IV]$

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

(c) (2 marks) What is the effect on the plain text of a one bit error in the transmission of an encrypted "block C_j"? How far the error propage?

One bit error in decrypted block P_j.

The error does not propagate.

continued on next page

This page is a blank page

END OF EXAMINATION