**Student Number** | |

The University of Melbourne

Department of Computing and Information Systems

# CRYPTOGRAPHY AND SECURITY

September, 2016

**Quiz Duration:** 45 minutes.

**Length:** This paper has **??** pages including this cover page.

**Authorised Materials:** None.

**Instructions to Students:** Answer all questions in this exam booklet.
Total marks for the test is 50. This is worth 10% 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.



*continued on next page*

1. (8 marks) Short Answer Questions (Please answer in the space provided).

   (a) Let $p$ be a prime number. Then for any $x$, $x^p$ $mod$ $p =$ $x$ .

   (b) $(15 + 17)$ $mod$ $26 =$ 6.

   (c) $11^{-1}$ $mod$ $12 =$ 11.

   (d) $2^{30}6^{2600}5^{33}$ $mod$ $7 = -1$.

   (e) $2^{144}3^{132}5^{100}$ $mod$ $4 = 0$.

   (f) $\phi(p_1\ p_2) = (p_1 - 1)(p_2 - 1)$.
   where $p_1$ and $p_2$ are distinct primes and $\phi$ is Euler's function.

   (g) All encryption algorithms are based on two general principles: substitution and permutation/transposition.

   (h) An active attack attempts to alter system resources or affect their operation.

 *continued on next page*

2. (7 marks) RSA Crypto system.

   (a) What are the hard mathematical problems on which security of RSA cryptosystem is based? You need to define the problems, not just the names.

      - **Factorisation.** Given $N$ a product of two large prime numbers, it is hard to factorise $N$.
      - **RSA Problem.** Given $C \equiv m^e \bmod n$, determine the $e^{th}$ root of $C$ modulo $n$, i.e. the message $m$.

   (b) Alice wants to configure her RSA parameters. She chooses two large random primes $p$ and $q$. Fill in the blanks in the following items which will help her compute the RSA parameters.

      i. Alice's RSA modulus $n$ is $pq$.

      ii. The encryption exponent $e$ is chosen such that $(e, \phi(n)) = 1$.

      iii. The decryption exponent d is found such that $de \equiv 1 \bmod \phi(n)$.

      iv. The ciphertext for the message m is $m^e \bmod n$.

 *continued on next page*

3. (6 marks)

(a) What are the two requirements of symmetric encryption?

- A strong encryption algorithm.
- A secret key known only to the authorised sender and receiver.

(b) Consider the following version of a variation of the classical cipher where plain text and cipher text elements are from integers 0 to 28. This alphabet is useful in representing 26 English characters and three more characters such as a blank, "," and the period ("."). The encryption function, which takes any plain text $p$ to a cipher text $c$, is given by

$$c = E_{(a,b)}(p) = (ap + b) \bmod 29,$$

where $a$ and $b$ are integers less than 29.

a. What is the decryption function for the scheme? $a^{-1}(c - b) \bmod 29$.

b. How many different non-trivial keys are possible for the scheme?

$28 * 29 - 1 = 811$.



*continued on next page*

4. (5 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.

   Inverse$a, n$ $g, x, y =$ XGCD$(a, n)$ $g = 1$ $x$ "doesn't exist." .

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

   i. $XGCD(12987, 46799) = 1, -13488, 3743$

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

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

   Now determine the inverse of the following numbers:

   i. $12 \mod 39$
   doesn't exist .

   ii. $12987 \mod 46799$
   $= (-13488) = 33311$ .

   iii. $17 \mod 29$
   $= 12$ .


*continued on next page*

5. ( 8 marks) For the prime numbers $p = 11$ and $q = 7$, calculate the RSA keys $e$ and $d$, satisfying the condition that $d$ has the smallest possible value.

$n = pq = 77$
$\phi(n) = (p-1)(q-1) = 60 = 2^2 \cdot 3 \cdot 5$
The smallest value for $d$ is 7.

$60 = 7 \times 8 + 4$
$7 = 4 \times 1 + 3$
$4 = 3 \times 1 + 1$
$3 = 1 \times 3 + 0$

$1 = 4 - (7 - 4 \times 1) \times 1$
$1 = 4 \times 2 - 7 \times 1$
$1 = (60 - 7 \times 8) \times 2 - 7 \times 1$
$1 = 60 \times 2 - 7 \times (16 + 1)$
$1 = 60 \times 2 + 7 \times (-17)$

So $e = -17 \equiv 43 \bmod 60$
i.e., $e$ is -17 or 43.



*continued on next page*

6. (6 marks) 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:

(a) What is the verification equation?

$(s)^e \stackrel{?}{\equiv} h(m) \bmod n$ .

(b) Describe the "second preimage resistant" property of the hash functions.

Given $x, h(x)$, it is impossible to determine $y$ such that $h(x) = h(y)$ .

(c) What is the consequence if the function $h$ used above satisfies all the requirements of cryptographic hash function except the second preimage resistant property?

If $h$ is not second preimage resistant then let $y$ be such that $h(y) = h(m)$. Then $(y, (h(m))^d)$ is a valid signature .

 *continued on next page*

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

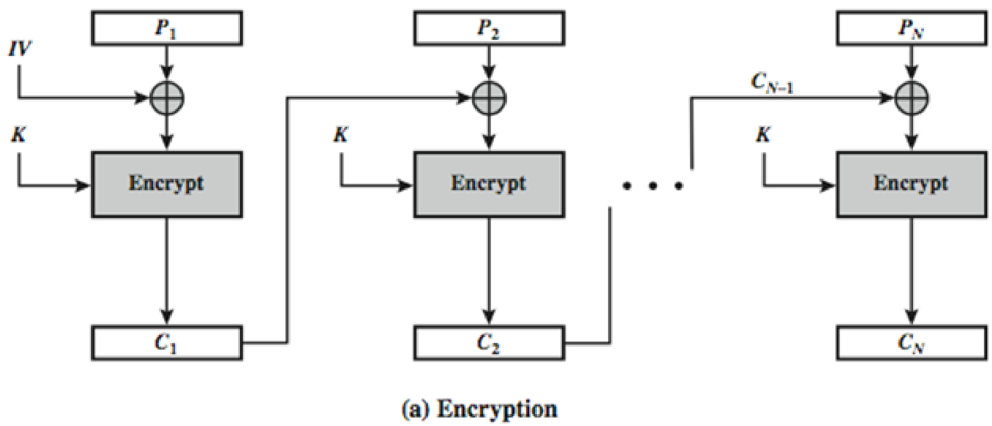


Figure 1: A Standard Mode of Encryption

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? CBC .

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

i. $IV =$ Initial value
ii. $K =$ Key
iii. $C_j =$ $j^{th}$ ciphertext block
iv. $P_j =$ $j^{th}$ plaintext block
v. $E_y[x] =$ Encryption of $x$ under key $y$

(c) Complete the equations for decryption below:

Decryption:
$P_1 =$ $D_K(C_1) \oplus IV$
$P_j =$ $D_K(C_j) \oplus C_{j-1} : j = 2, \ldots, N$

(d) What is the effect on the plain text of a one bit error in the transmission of an encrypted "block $C_j$"? $P_j$ and $P_{j+1}$ will be affected.

 *continued on next page*

8. (3 marks) Consider the finite field $GF(8)$ as discussed in class:

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

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

(a) What is the multiplicative inverse of $x^2$? $x^5 = 1 + x + x^2$ .

(b) Compute $x + x^2 + x^4$. $0$ .

(c) Compute $x^3 + x^6 + x^5$; $1$ .

**END OF EXAMINATION**