Student Number SOLUTION

The University of Melbourne

Department of Computing and Information Systems

CRYPTOGRAPHY AND SECURITY

September, 2017

Quiz Duration: 45 minutes.

Length: This paper has 7 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. (10 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 mod p......

(b) $(15 - 19) \mod 26 =$ ......22......

(c) $17^{-1} \mod 18 =$ ......17 or -1......

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

(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 ϕ is Euler's function.

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

(h) The minimum positive integer x that satisfies the following relations is 23

$x = 2 \mod 7$;
$x = 3 \mod 5$.

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

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

continued on next page

2. (8 marks) RSA and Public Key Crypto systems.

(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.

① integer factorisation

hard to factorise a large integer into product of primes

② RSA problem

given C and e, hard to find M where $C = M^e \bmod n$

(b) What are the hard mathematical problems on which security of Diffie-Hellman Key Agreement protocol is based? You need to define the problems, not just the names.

① discrete logarithm

let $g^x = y$, it is hard to solve x knowing g and y

② computational Diffie-Hellman problem

given g, g^a, g^b it is hard to find g^{ab}

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 $\gcd(e, \varphi(n)) = 1$.

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

iv. The ciphertext for the message m is m^e mod n.

 continued on next page

3. (12 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)
    if g==1
          return x
    else
       "no inverse"
```

(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 N/A

ii. 12987 mod 46799 -13488 or 33311

iii. 17 mod 29 12

iv. 12 mod 17 10

 continued on next page

4. (10 marks) For the prime numbers $p = 11$ and $q = 7$, calculate the non-trivial RSA keys e and d, $e > 1$, satisfying the condition that d has the smallest possible values.

$n = pq = 77$

$\varphi(n) = \varphi(p)\varphi(q) = 10 \times 6 = 60$

$d = 7$

$60 = 8 \times 7 + 4$

$7 = 1 \times 4 + 3$

$4 = 1 \times 3 + 1$

$1 = 4 - 1 \times 3$

$1 = 4 - 1 \times (7 - 1 \times 4)$

$1 = 2 \times 4 - 1 \times 7$

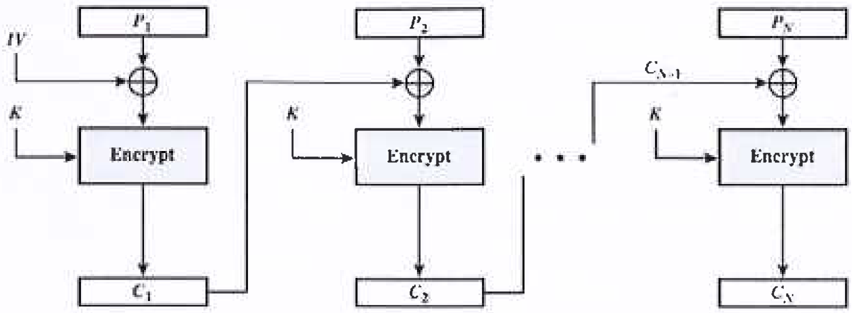
$1 = 2 \times (60 - 8 \times 7) - 1 \times 7$

$1 = 2 \times 60 - \underline{17} \times 7$

$e = +43$

 continued on next page

5. (10 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?

Cipher Block Chaining

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

i. $IV =$ ....initialisation vector

ii. $K =$ ....secret key

iii. $E_y[x] =$ ....encryption function on x with key y

(c) Complete the equations for decryption below:

Decryption:

$P_1 =$ ________. $D_K[C_1] \oplus IV$

$P_j =$ ________. $D_K[C_j] \oplus C_{j-1}$ $j \geq 2$

(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 1 bit of P_{j+1}

END OF EXAMINATION