Student Number_____________

THE UNIVERSITY OF MELBOURNE
DEPARTMENT OF COMPUTING AND INFORMATION SYSTEMS

Quiz – Practice

COMP90043 Cryptography and Security

Duration: 45 minutes

Authorized materials:
The following items are authorized: writing materials (e.g. pens, pencils) and non-electronic dictionaries are allowed.
Calculators and all other books are *not* allowed.

Instructions to Students:

- Attempt all questions.

PART I: True or False (Put an X in the appropriate column)

A) The Euclidean algorithm cannot be adapted to find the multiplicative inverse of a polynomial.
   B) True
   B) False

B) A prime concern with DES has been its vulnerability to brute-force attack because of its relatively short key length.
   C) True
   C) False

C) Confusion seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key.
   D) True
   D) False

D) The way to measure the resistance of a hash algorithm to cryptanalysis is to compare its strength to the effort required for a brute-force attack.
   E) True
   E) False

E) A recipient in possession of the secret key cannot generate an authentication code to verify the integrity of the message.
   F) True
   F) False

PART II: Multiple Choice Questions (Please put an X for the correct answer)

A) An important quantity in number theory referred to as __________ , is defined as the number of positive integers less than n and relatively prime to n.
   B) CRT
   B) Miller-Rabin
   B) Euler’s totient function
   B) Fermat’s theorem

B) __________ is when each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.
   C) Substitution
   C) Diffusion
   C) Streaming
   C) Permutation

C) The __________ indicates that the subscriber identified in the certificate has sole control and access to the private key.
   D) OAEP
   D) Public Key Certificate
   D) Digital Signature
   D) PKI

D) Confidentiality can be provided by performing message encryption __________ the MAC algorithm.
   E) before
   E) before or after
   E) after
   E) during

E) The key used in symmetric encryption is referred to as a __________ key.
   F) public
   F) secret
   F) private
   F) decryption

PART III: Fill in the Blanks Questions (Please answer in the left column)

- Two numbers are ______________ if their greatest common divisor is 1.

- In _______________, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits.

- A _____________________ is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy, whereas the calculation of the inverse is infeasible.

- A ___________________________ is an attack in which the adversary chooses a number of ciphertexts and is then given the corresponding plaintexts, decrypted with the target's private key.

- When a hash function is used to provide message authentication, the hash function value is often referred to as a _________________.

PART IV: Short Answer Questions (Please answer in the space provided)

Calculate using modular arithmetic (Show your work)

1. 2^{123} mod 29 = ___________________

2. -1298 mod 12 = ______________________

3. 5^{31} mod 31 = ______________________

Calculate Euler's totient function for the following numbers (Show your work)

1. 1653 = _________________

2. 2^7 = ___________________

Given the following RSA parameters, compute the missing parameters (Show your work)

Public Key = (3, 15), C = 2, M = ______________

Answer the following (Show your work if applicable)

1. 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

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

where *a* and *b* are integers less than 26.

a. What is the decryption function for the scheme?

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