PENINSULA COLLEGE GEORGETOWN

FINAL SEMESTER EXAMINATION

Programme	:	**DIPLOMA IN COMPUTER SCIENCE**
Course	:	**CRYPTOGRAPHY**
Course Code	:	**DCS2133**
Duration	:	**3 Hours**

INSTRUCTIONS TO CANDIDATES:

1. Please read the instructions given in the question paper **CAREFULLY.**
2. This question paper consists of **FOUR (4)** questions
3. Answer **ALL** questions in the question paper.
4. Answers to the questions are to be written into the examination booklet.
5. Electronic dictionaries, lecture notes, files or any unauthorized materials except writing equipment are strictly prohibited.

This question paper must be submitted along with all used and/or unused rough papers and/ or graph papers (if any). Candidates are **NOT ALLOWED** to take any examination paper(s) used or unused out of the examination hall.

WARNING:

The Examination Board of Peninsula College Georgetown regards cheating as a very serious offence and will not hesitate to mete out the appropriate punitive actions according to the severity of the offence committed, and in the accordance with the clauses stipulated in the Students' Handbook, up to and including expulsion from Peninsula College Georgetown.

(*This booklet contains* **3** *printed pages including this page*)

For examiner's use only

QUESTION NO.	MARKS
1	/ 25
2	/ 25
3	/ 25
4	/ 25
Total	**/ 100**

Answer **ALL FOUR (4)** questions on the separate sheet provided. **[100 marks]**

1. a) ExpressMail wants every email to be authenticated and protected from modification or tampering while it is in transit from the sender to the receiver. Suppose Alice is sending an email M to Bob.

The following are ExpressMail's design constraints, which of the following options would be a secure way to protect the authenticity and integrity of her email? Justify your answer.

i. Alice's software should encrypt M under Bob's public key. In other words, Alice's software should send E*KB (M)* to Bob. (5 marks)

ii. Alice's software should choose a new symmetric key k for this email, send an encryption of *k* under Bob's public key, and also send an encryption of *M* under *k* using a stream cipher such as RC4. In other words, Alice should send *EKB (k),* and *M* ⊕RC4(*k*). (5 marks)

b) Give **TWO (2)** differences between the handwriting signature and digital signature. (5 marks)

c) Explain why randomness is needed in cryptography. (4 marks)

d) Determine the following randomness approach with **ONE (1)** example each.

i) Deterministic (3 marks)
ii) Non-Deterministic (3 marks)

Total: [25 Marks]

2. A common security objective is to send a message from Alice to Bob in such a way that nobody else can read the message and Bob can be sure the message he received did indeed come from Alice.

a) Determine **FOUR (4)** goals of a simple cryptographic protocol to meet this security objective. (12 marks)

b) Illustrate a protocol based on Protocol 1, which, in addition to the existing protocol goals, also allows Alice to confirm Bob is alive. (7 marks)

c) Identify **TWO (2)** better responses would be to repair the reflection attack feasible in Protocol 3. Justify your answer. (6 marks)

Total: [25 Marks]

3. a) Explain the following categories of identification information and provide **TWO (2)** examples of each category.
   i. Something that claimant has. (3 marks)
   ii. Something that the claimant is. (3 marks)
   iii. Something that the claimant knows. (3 marks)

b) Determine **ONE (1)** problem that might arise if we base a freshness mechanism on the suggested component:
   a) An inaccurate clock (3 marks)
   b) A sequence number that regularly cycles around (3 marks)
   c) A nonce that is randomly generated from a small space. (3 marks)

c) State **SEVEN (7)** elements include in the X.509 standard. (7 marks)

Total: [25 Marks]

4. a) Identify **TWO (2)** possible plaintext attacks on the RSA algorithm with justification. (10 marks)

b) Explain any **THREE (3)** techniques of Public - Key Distribution (9 marks)

c) State **SIX (6)** cryptography application environments. (6 marks)

Total: [25 Marks]

- END OF QUESTIONS -