PENINSULA COLLEGE
GEORGETOWN

FINAL EXAMINATION

Programme Name	:	**DIPLOMA IN COMPUTER SCIENCE**
Course Code & Name	:	**DCS2133 CRYPTOGRAPHY**
Duration	:	**3 HOURS**

INSTRUCTIONS TO CANDIDATES:

1. Please read the instructions given in the question paper **CAREFULLY.**
2. The 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 unauthorised 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*)

DO NOT OPEN THIS BOOKLET UNTIL YOU ARE ALLOWED TO DO SO

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

1. a) SecureSend, a leading email service provider, places paramount importance on data security and integrity. They have stringent measures in place to ensure that every email sent through their platform is protected against unauthorized access and tampering. In this scenario, Alice intends to send a crucial email (M) to Bob, and SecureSend employs specific design constraints to guarantee the authenticity and integrity of the email. Provide your comment based on the schemes below and 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* $\oplus$RC4(*k*). (5 marks)

   b) What are **TWO (2)** differences between a handwritten signature and a 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 prevalent security goal is to securely transmit a message from Alice to Bob, ensuring confidentiality so that only Bob can read the message, and authentication, guaranteeing that the message originates from Alice.

   a) Identify **FOUR (4)** objectives of a basic cryptographic protocol designed to fulfill this security requirement. (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)** improved responses to address the feasibility of a reflection attack in Protocol 3 and justify your answer for each response. (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:

i) An inaccurate clock (3 marks)

ii) A sequence number that regularly cycles around (3 marks)

iii) A nonce that is randomly generated from a small space. (3 marks)

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

Total: [25 Marks]

4. a) Explain **FOUR (4)** techniques proposed for the distribution of public keys. (12 marks)

b) Determine **TWO (2)** aspects to use public-key encryption. (4 marks)

c) Explain **THREE (3)** cryptographic applications that you know. (9 marks)

Total: [25 Marks]

- END OF QUESTIONS -