CANDIDATE: please attach Student Support Unit sticker, if relevant.

THE UNIVERSITY OF SUSSEX

BSc and MComp THIRD YEAR EXAMINATION

Introduction to Computer Security
G6077

If you have extra time due to Reasonable Adjustments this is additional to the exam duration below and has been added to your assessment on Canvas.

Date: Thursday, 11 January 2024
Start: 9.30
Exam Duration: 2.5 hours (including 30 minutes for scanning, collating, uploading)

Candidates should answer TWO questions out of THREE.

If all three questions are attempted only the first two answers will be marked.

Each question is worth 50 marks.

Write or type your answers on A4 paper, scan and save as a single PDF file and upload to Canvas

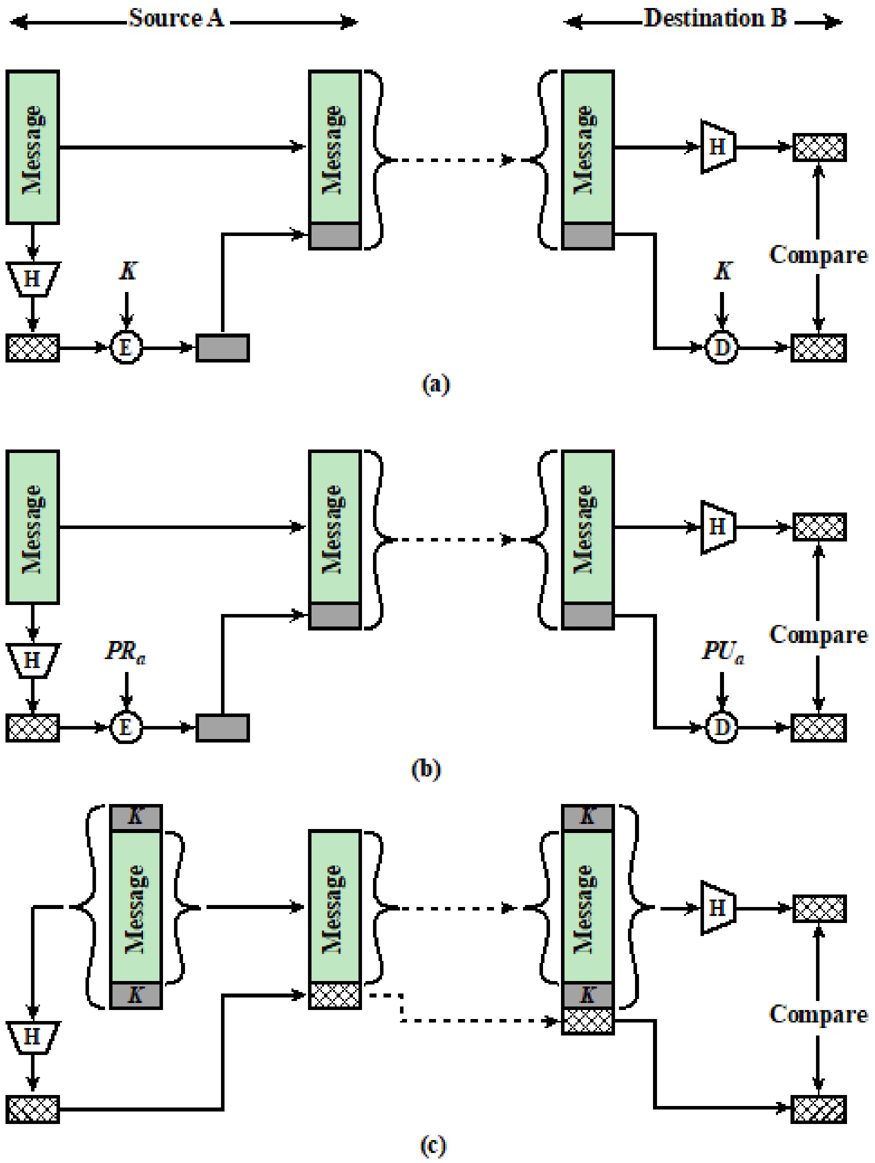
Please make sure that your submission includes the following:
Your candidate number (Do not put your name on your paper)
The title of the module and the module code

Read Academic Integrity Statement

You MAY access online materials, notes etc. during this examination. You must complete this assessment on your own and in your own words. DO NOT discuss this assessment with others before the end of the 2.5 hour window. By submitting this assessment you confirm that your assessment includes no instances of academic misconduct, for example plagiarism or collusion. Any instance of academic misconduct will be thoroughly investigated in accordance with our academic misconduct regulations.

1. Nowadays, many computer security services and applications use cryptographic algorithms as one of their most important element.

   a) Consider the image below.



i. Briefly describe the schemes illustrated.

[15 marks]

ii. Which scheme among them is less costly computationally? Justify your answer.

[5 marks]

b) Which asymmetric encryption algorithm is becoming more suitable nowadays for online applications such as electronic commerce? Justify your answer.

[5 marks]

c) Consider the following statement: “A digital envelope is encrypted twice”.

i. Explain what makes digital envelopes secure.

[10 marks]

ii. Which security requirements does it provide?

[5 marks]

d) Which security mechanisms are used to protect *data at rest*? Justify your answer.

[10 marks]

2. The need for database security is due to the fact that organisational databases concentrate sensitive information in a single logical system.

a) Explain how Attribute Based Access Control can be used to enforce Database Security. Justify your answer with an example.

[15 marks]

b) Explain how malicious code could be injected into a cookie to perform SQLi attacks.

[10 marks]

c) Are SQLi attacks covered by the Computer Misuse Act 1990? Justify your answer.

[10 marks]

d) Explain how the Plan-Do-Check-Act process model can be used to manage database security risk.

[15 marks]

/Turn over

3. Many organisations have massively adopted computing paradigms over the last two decades due to their numerous benefits.

a) Consider the following statement: “Availability and auditability are major concerns in Cloud Computing”. Explain how they are addressed, considering the essential characteristics of the cloud.

[15 marks]

b) Consider the following statement: “*Data at rest* is one of the pillars of Cloud Computing.”

i. Explain how data protection is ensured. Give an example of an application and explain how this is guaranteed.

[15 marks]

ii. Is Cloud Security as a Service an alternative solution to the *data at rest* problem? Justify your answer.

[10 marks]

c) Explain the advantages/disadvantages of Fog Computing from a security point of view. Justify your answer.

[10 marks]

End of paper