IN-COURSE ASSESSMENT (ICA) SPECIFICATION

Module Title: **System Administration and Security**	Module Leader:
	Module Code:
Assignment Title: **Cryptography basics, security analysis, design and implementation**	Deadline Date:
	Deadline Time:
	Submission Method:

FULL DETAILS OF THE ASSIGNMENT ARE ATTACHED
INCLUDING MARKING & GRADING CRITERIA

System Administration and Security SAS

Introduction

This assessment includes two parts:

- Part I involves a set of short questions on the topic of cryptography and will consider the correctness and completeness of the solutions and your understanding of the concepts and will assess learning outcomes PTS1, PKCS3, PKCS4.
- Part II involves written design exercises and will addess learning outcomes PTS1, PTS2, PKCS3, PKCS4, PKCS5, PKCS6, PKCS7. You are required to analyse three scenarios, select and justify appropriate security techniques as part of solving the problem in the scenarios, deign/implement the solution, and communicate that design as a written report, including rationales, comparisons and alternatives. The use of security related terms and the demonstration of relevant legal, social, ethical and professional issues is included where needed.

You must submit original work written by yourself, you must not share your work with your classmates. If you submit multiple attempts, then I will mark the last submission received before the deadline, or if no submissions are received before the deadline, the submission received first after the deadline will be marked. If you hand in late, I will only mark within 7 days and your work will be capped to a pass.

Part I Cryptography questions (25%)

Basic concept

1. Explain the difference between symmetric and asymmetric encryption. Describe a method of asymmetric encryption, and discuss the vulnerabilities of it.

[5 marks]

Simple encryption and decryption

2. Decrypt **OHW PHR XWC CC** using the Caesar cipher (shift of **3**).

[5 Marks]

RSA

3. Assume a public key for RSA encryption given by the pair (143,11). Find the private key corresponding to this pair.

[5 marks]

4. Using the pair (143, 11), decode the encrypted message (111 4 88 57 116 67) assuming the letters were represented by ASCII values

(recall that the ASCII values are 65->A, 66->B, … and 97->a, 98->b, …)

[5 marks]

Diffie-Hellman protocol

5. Describe in detail the Diffie-Hellman protocol for ***three*** parties Alice, Bob and Carol.

[5 Marks]

Part II Security analysis and design (75%)

Scenario I - Security models [20 Marks]

MGB Ltd. is a company providing security solutions to public services. You are asked to help the MGB Ltd to design a security model for the national defence department - a part of an e-government project on secure information control in managing troops. Assume the armed forces be classified as: {*army, navy, air force, marines*}, the security levels are typed as: {high, low}.

Your tasks: You should produce a short report (around 500 words) to formalise a Bell Lapadula model to address the confidentiality properties for the specified scenario, and to discuss the strength and weakness of your model.

*Hint: You need to describe the model (specify subjects, objects, possible operations – which can be flexible, design your own but need to show your understanding of specifying and applying the BLP model in a real case), the security lattice (a graph can be helpful), the policy and the security properties for the **given scenario** above*.

Scenario II - Security Analysis and Solutions to Conference Management Systems [25 Marks]

A conference manage system is a web-based management system which allows researchers submit research papers, the program committee (PC) members (reviewers) to browse papers and contribute reviews, scores and discussion, and release decisions (such as rejection or accept) via the Web. In one arrangement, the conference chair downloads and hosts the appropriate server software. (A good example is easychair: https://easychair.org/conference)

The system allows users to submit papers, enter reviews & scores and access reviews & scores associated with events (conferences or workshops) regarding to the role of the uses. A user is granted access to the system by providing a role (chair, reviewer, or author) along with a user-id and associated password. Permissible roles for each user are specified at the time a new event is added to the management system. Reviews & scores on papers are initially assigned by chairs (chairs assign papers to reviewers for reviewing, one reviewers can be assigned multiple papers, one paper can be allocated to multiple reviewers). Reviewing are done by reviewers. And a chair can perform any and/or all of these actions, but a chair's updates can only be changed by the chair. An author, in addition to learning about his or her reviews & grades on individual papers, is entitled to learn the acceptance statistics (but not other papers' reviews), and the conference program.

Threat model: The adversary is a user who desires to learn the reviews & scores, changes reviews & scores, or prevent others from learning or changing reviews & scores. The adversary has access to the management system and also can read, delete, and/or update network messages in transit. The adversary cannot physically access or run programs on a user's machine that is running a browser to access the management system. And the adversary can not physically access or run programs on the server hosting the management system.

Your tasks: You are asked to produce a report (1500-2000words) to provide contemplate descriptions of the above Web-based Conference Management System. You should address the following issues:

1. Demonstrate a broad understanding of the professional, ethical and legal compliance considerations around network security.
2. Analyse a range of security concepts, security models, principles and practice in an appropriate environment.
3. Evaluate potential secure infrastructures to meet an appropriate system requirement.

4. Select and justify appropriate security techniques to meet an appropriate system requirement.
5. Operate ethically in order to implement and test a secure infrastructure to meet an appropriate business requirement.
6. Communicate effectively and professionally in writing.

Hint: Assuming that the manager is not a technical person, craft your explanation in a way that can be explained to a layman and include figures where necessary. You could think about:

- *Assets and security properties: what objects should be protected, what security properties might we expect the system to enforce? For each such security property, label it with one of: confidentiality, integrity, or availability?*
- *Vulnerability: explain the vulnerability in the system and use an attack tree/model to describe how an attack could be mounted. Restrict your consideration to the threat model provided.*
- *Protection: what cost-effective protections are available against the threats that you identify. Remember the focus is on software vulnerabilities.*

Scenario III- Design and Implementation of a Secure Network [30 marks]

This task involves designing and implementing an Internet-connected secure network for a medium-sized company requiring 500 machines named Smith Logistics, UK. They want to implement a secure network that uses Class C network address with multiple subnets – They have asked you for a price quote as well. But they want to see a packet tracer implementation and simulation results before they commit to purchasing anything.

You can use Packet tracer/Opnet/Omnet++ for the implementation and security measures. The implementation of the network should consist of core, distribution and access layer.
It should use a minimum of two routers at the distribution and a further 2-4 for the core layer. All router interfaces must be tested for the correct subnet operations.

Your tasks: You should write a report with the appropriate design and implementation solution (2500 words max, but flexible) documenting all that you have done, including how the network is set up. Use the tasks below as a guideline to write.

1. Using a drawing tool of your choice design the network. Draw a simple network diagram of your network.
   Hints: Design the logical diagram. You can ignore the device location in a logical design. Use Visio or any drawing tool for the diagram. Don't forget to label the diagram core, access and distribution layer.

2. Design and Implement an IPv4 subnetting scheme. You can use any address in class c.

3. Hint: Test a small subsection of the network before implementing the full addressing scheme in packet tracer.

4. The report must describe the design and all of the decisions that you have made in the process of developing the design. This will include a discussion of the design model, Security, WAN protocol, Layer 2, 3 and wireless protocols that you have decided to use. *Hint:* Restrict your discussion to the main layer 1,2 and 3 protocols

5. Show the detailed cost of implementing your solution in a table format. You can try to show two different costs for the company to choose from.
   Hints: Research on the costs of servers (hardware and software), switches, workstations, cables, etc.

6. Show all references used in the report, using appropriate referencing.
   Hints: Harvard referencing can be used and make sure the format is fully followed.

Advice and assistance

Consult the module tutors during a scheduled session or email the module tutors.

Learning outcomes to be assessed (details see assessment criteria)

1. [PTS1] Communicate complex issues in cybersecurity and system administration to both specialist and non-specialist audiences.
2. [PTS2] Evaluate, select and use effectively appropriate security and system administration tools.
3. [PKCS3] Demonstrate a comprehensive and critical understanding of concepts, theories and issues relating to cybersecurity and system administration.
4. [PKCS4] Research, evaluate and implement modern cybersecurity and cryptography techniques.
5. [PKCS5] Integrate and synthesise diverse knowledge, evidence, concepts, theory and practice in system administration, including security issues, to solve problems.
6. [PKCS6] Provide detailed arguments and present conclusions about system administration and security issues, including scenarios with limited or inaccurate information.
7. [PKCS7] Demonstrate an awareness of ethical conduct in systems administration and cybersecurity scenarios.

Assessment criteria

The criteria below is necessarily incomplete as we cannot anticipate every possible ICA submission.

Grade Part I (25) **Learning Outcomes to be assessed: RKCS3, PKCS4**	
Q1 (5)	Understanding of the concepts
Q2 (5)	correctness
Q3 (5)	5 marks for correct solutions of the private key and details provided; if correct p is given: 2 marks; if correct q is given: 2 marks.
Q4 (5)	5 marks for correct decrypt message and details provided; 4 marks if understanding shown but final computation is incorrect, 1 mark for one correct part of the message.
Q5 (5)	Correctness and completeness

Grade Part II : scenario I (20) **Learning Outcomes to be assessed: PTS1, PTS2, PKCS3, PKCS5, PKCS6**	
State machine (5)	Sound description of the model
Security lattice (5)	Correct description on the partial ordering of the security labels
Security properties (5)	Reasonability and completeness of the description
Strength and weakness (3)	Reasonability and completeness of the description
Writing and reference (2)	

Grade Part II: scenario II (25) **Learning Outcomes to be assessed: PTS1, PTS2, PKCS3, PKCS5, PKCS6, PKCS7**	
70-100%	*Excellent* [SYNTHESIS] Demonstrate a broad understanding of the professional, ethical and legal compliance considerations around network security, and an excellent understanding of modern information and network security properties and system threat & vulnerabilities is demonstrated with excellent links to the specified scenario. There is clear evidence of work beyond taught material. [DESIGN] An excellent analysis of security protection techniques and their application is demonstrated in relation to the specified scenario. There is clear evidence of work beyond taught material. [WRITE] A very clear and readable report, with excellent structuring, good use of grammar and referencing. Document submitted as PDF.

60-69%	*Substantially correct/appropriate (based on taught material & module requirements)* [SYNTHESIS] Demonstrate a good understanding of the professional, ethical and legal compliance considerations around network security, a very good understanding of modern information and network security properties and threats is demonstrated with clear linkage to the specified scenario. [DESIGN] A very good analysis of security protection techniques and their application is demonstrated in relation to the specified scenario.

	[WRITE] A clear and readable report, with appropriate structuring and referencing. Document submitted as PDF.
50-59%	*Minor errors/omissions/issues* [SYNTHESIS] Demonstrate a reasonable understanding of the professional, ethical and legal compliance considerations around network security, and a generally/mostly good understanding of modern information and network security properties and threats is demonstrated with clear linkage to the specified scenario. [DESIGN] A generally/mostly good analysis of security protection techniques and their application is demonstrated in relation to the specified scenario/task. [WRITE] A clear and readable report, with minor errors in writing, structure or referencing. Document submitted as PDF.
40-49%	*Major errors/omissions/issues* [SYNTHESIS] Demonstrate a limited understanding of the professional, ethical and legal compliance considerations around network security, an a limited understanding of modern information and network security properties and threats is demonstrated and/or limited linkage to the specified scenario. [DESIGN] A limited analysis of security protection techniques and their application is demonstrated in relation to the specified scenario/task. [WRITE] A report, with major issues of writing, structure or referencing. Document submitted as PDF.

30-39%	Unsatisfactory [SYNTHESIS] Demonstrate a vert limited understanding of the professional, ethical and legal compliance considerations around network security, and a very limited understanding of modern information and network security properties and threats is demonstrated. [DESIGN] A very limited analysis of security protection techniques and their application is demonstrated. [WRITE] A report that is difficult to read or comprehend but includes some attempt at structure and referencing OR document is not submitted as a PDF.
0-29%	*Inadequate* [SYNTHESIS] Demonstrate little understanding of the professional, ethical and legal compliance considerations around network security, and little to nothing demonstrated in relation to modern information and network security properties and threats. [DESIGN] Little to no analysis of security protection techniques and their application. [DESIGN] A report that is very difficult to read and comprehend, and makes no attempt at referencing.

Grade Part II: scenario III (30) **Learning Outcomes to be assessed: PTS2 , PKCS3 and PKCS5**	
Task 1 (12)	Network Design and Implementation (6 marks); IP and subnetting (6 marks);
Task 2 (8)	Discussion of the relevant protocols and hardware used to design this network and How the protocols meet the requirements.
Task 3 (7)	Cost of implementation
Task 4 (3)	Professional writing and good use of reference.