**IN-COURSE ASSESSMENT (ICA) SPECIFICATION**

|  |  |  |
| --- | --- | --- |
| Module Title:  **Network and Systems Security** | Module Leader: | **Dr. Nauman Israr** |
| Module Code: | **CIS-4069-N** |
| Assignment Title:  **Cryptography basics, Security Analysis, Design and Implementation** | Submission Deadline: 6 Aug 2025  Feedback Date: **5 Sept 2025** | |
| Deadline Time: | **4:00 pm** |
| Submission Method:  **Online (Blackboard Ultra)** | |

**Online Submission Notes:**

* Please follow carefully the instructions given on the Assignment Specification
* When Extenuating Circumstances (e.g. extension) has been granted, a fully completed and signed Extenuating Circumstances form must be submitted to theSchool Reception or emailed to [scdt-assessments@tees.ac.uk](mailto:scdt-assessments@tees.ac.uk).

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

**Network and Systems Security**

(CIS4069)

# Part 1: General Cryptography Questions (25%)

**Simple encryption and decryption [10 Marks]**

1. Using the Vigenere (polyalphabetic) cipher, encrypt your **full name** (no space between first and last

name, you may include your father's name, too) using your **city name**. [5 marks] For example, **BlaisedeVigenere**, key **Paris.** Explain the process briefly**.**

1. Using the Playfair cipher, encrypt the following text. Use your name as the key and consider 'M' and

'N' as one letter. [5 marks]

Text: **THIS IS A MESSAGE**, For example, key: **Rachel**

Explain the process briefly.

# RSA [10 Marks]

1. Give the three scenarios from your studies at Teesside University where RSA could

be used. [5 marks]

1. Is achieving all three, Confidentiality, Data Integrity and Authentication, together in asymmetric cryptography? Justify your answer using an appropriate diagram. [5 marks]

# Diffie-Hellman Protocol [5 Marks]

1. Describe the Diffie-Hellman protocol for ***three*** parties Alice, Bob and Carol. [5Marks]

# Part 2: Security Analysis (75%)

**Scenario 1: Security models [20 Marks]**

ABC Ltd. is a company providing security solutions to public services. You are asked to help ABC Ltd design a security model for the national defence department, 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 formalize a Bell Lapadula model to address the confidentiality properties for the specified scenario and discuss your model's strengths and weaknesses.

*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 identifying 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 2: Security Analysis and Solutions to Conference Management Systems [25 Marks]

A conference management system is a web-based management system which allows researchers to submit research papers to the program committee (PC) members (reviewers) to browse documents and contribute reviews, scores and discussion, and release decisions (such as rejection or acceptance) via the Web. The conference chair downloads and hosts the appropriate server software in one arrangement. (A good example is the easy chair: [https://easychair.org/conference)](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 the role of the users. A user can access the system by providing a role (chair, reviewer, or author), user ID, and associated password. Permissible roles for each user are specified when 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 reviewer can be assigned multiple papers, and one paper can be allocated to multiple reviewers). Reviewing is done by reviewers. 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 know 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, change reviews & scores, or prevent others from learning or changing reviews & scores. The adversary has access to the management system and can read, delete, and/or update network messages in transit. The adversary cannot physically access or run programs on a user's machine running a browser to access the management system. The adversary cannot physically access or run programs on the server hosting an agreement system.

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

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

*Hint: Assuming that the manager is not a technical person, craft your explanation in a way that can be explained to a non-specialist and include figures where necessary.*

# Scenario 3: 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 1200 machines, Smith Logistics UK. They want to implement a secure network that uses a Class B network address with multiple subnets – They have also asked you for a price quote. However, they want to see 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 a 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, but flexible) documenting everything 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 diagrams. Don't forget to label the diagram core, access and distribution layer.*

1. Design and Implement an IPv4 subnetting scheme. You can use any address in class C/B.

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

1. The report must describe the design and all the decisions you have made to develop the plan. The discussion should also address the design model, WAN protocol, security risks, and mitigations at Layers 1, 2 and 3 of the TCP/IP stack.

*Hint:* Restrict your discussion to the main layer 1,2 and 3 protocols

1. Show the detailed cost of implementing your solution in a table format. You can try to show the company two different costs.
2. The report must describe the legal issues and ethical conduct in managing the proposed network.

*Hints: Research the cost of servers(hardware and software), switches, workstations, cables, etc.*

Show all references used in the report using *Harvard* referencing.

**Note of the use of AI Tools**: You can use AI tools to learn a concept used in the ICA, but remember, copy-paste of the solution by AI is not allowed. Always write the report yourself and reference all your sources to find the solution.

# Deliverable and deadline

You should submit your report as a PDF document via the VLE by the deadline on the front cover.

# Advice and Assistance

If have any queries or need help, please consult the module leader/tutor.

**Assessment Criteria**

|  |  |
| --- | --- |
| **Part 1: General Questions (25) – 5 marks for each question** | |
| **Q1** | correctness |
| **Q2** | correctness |
| **Q3** | 5 marks for correct solutions of the private key and details provided; if correct p is given: 2 marks;  If the correct q is given, two marks will be given. |
| **Q4** | 5 marks for correct decrypt message and details provided;  4 marks if understanding is shown but the final computation is incorrect, one mark for one correct part of the message. |
| **Q5** | Correctness and completeness |

|  |
| --- |
| **Part 2: Scenario 1 (20)** |
| * **State machine:** Sound description of the model (5) * **Security lattice:** Correct description of the partial ordering of the security labels (5) * **Security properties:** Reasonability and completeness of the description (5) * **Strength and weakness:** Reasonability and completeness of the description (3) * **Writing and reference:** Appropriate writing style and referencing (2) |

|  |  |
| --- | --- |
| **Part 2: Scenario 2 (25)** | |
| **75%/85%/95%** | *Excellent*  An excellent understanding of modern information and network security properties and system threats & vulnerabilities is demonstrated with excellent links to the specified scenario. There is clear evidence of work beyond the taught material.  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 the taught material.  A clear and readable report, with excellent structuring and good use of grammar and referencing. Document submitted as PDF. |

|  |  |
| --- | --- |
| **65%** | Substantially correct/appropriate (based on taught material & module requirements)  A good understanding of modern information and network security properties and threats is demonstrated with clear linkage to the specified scenario.  A very good analysis of security protection techniques and their application is demonstrated in relation to the specified scenario.  A clear and readable report with appropriate structuring and referencing. Document submitted as PDF. |
| 55% | Minor errors/omissions/issues  A generally/mostly good understanding of modern information and network security properties and threats is demonstrated with clear linkage to the specified scenario.  A generally/mostly good analysis of security protection techniques and their application is demonstrated in relation to the specified scenario/task.  A clear and readable report with minor errors in writing, structure or referencing. Document submitted as PDF. |
| **45%** | Major errors/omissions/issues  A limited understanding of modern information and network security properties and threats and/or limited linkage to the specified scenario is demonstrated.  A limited analysis of security protection techniques and their application is demonstrated in relation to the specified scenario/task.  A report with significant issues of writing, structure or referencing. Document submitted as PDF. |
| **45%** | Major errors/omissions/issues  A limited understanding of modern information and network security properties and threats and/or limited linkage to the specified scenario is demonstrated.  A limited analysis of security protection techniques and their application is demonstrated in relation to the specified scenario/task.  A report with significant issues of writing, structure or referencing. Document submitted as PDF. |
| **35%** | Unsatisfactory  A minimal understanding of modern information and network security |

|  |  |
| --- | --- |
|  | Properties and threats are demonstrated.  A minimal analysis of security protection techniques and their application is demonstrated.  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. |
| **20%** | Inadequate  Little to nothing is demonstrated in relation to modern information and network security properties and threats.  Little to no analysis of security protection techniques and their application.  A report that is very difficult to read and comprehend and makes no attempt at referencing. |

|  |  |
| --- | --- |
| **Part 2: Scenario 3 (30)** | |
| **Task 1 (12)** | Network Design and Implementation, including DMZ and IDS systems (6 marks); IP and subnetting (6 marks); |
| **Task 2 (8)** | Discuss the protocol's security risks and mitigation and how the protocols meet the requirements. |
| **Task 3 (7)** | Cost of implementation |
| **Task 4 (3)** | Professional writing and good use of reference. |