Department of Information Technology
Faculty of Computing
Sri Lanka Institute of Information Technology

IE3082: Cryptography

Year 3 Semester 2

2025

Assignment Title	Information Security Risk Management Assignment
Learning outcomes covered	LO1: Evaluate cryptographic requirements in computer systems and networks.LO3: Evaluate information security risks against business requirements and propose mitigation techniques. LO3: Differentiate approaches used in modern crypto schemes. LO4: Evaluate different approaches of cryptanalysis.
Assignment Mode	Report Submission & Viva
Maximum Marks	100
Contribution to the Final Grade	20%
Date published	Week 6
Deadline for submissions	Week 11
Mode of Submission	Report Submission (PDF)

Objective: The objective of this assignment is to evaluate the performance and other aspects of selected cryptographic algorithms within a 4-week period. This will help students develop a practical understanding of how different algorithms perform under various conditions and their suitability for specific applications.

Assignment Description: Students will work in groups of 5 to evaluate a selected set of cryptographic algorithms, including at least one symmetric key algorithm, one asymmetric key algorithm, and one hash function. The assignment will focus on both theoretical analysis and practical implementation.

The assignment is broken down into four key phases, each aligned with a specific week of the timeline.

Week 8: Algorithm Selection and Research

Task:

- Select the cryptographic algorithms to be evaluated. Each group should choose at least:

- One symmetric key algorithm (e.g., DES, AES, 3DES, Blowfish, Twofish, RC4, RC5, RC6,ChaCha20, IDEA).
- One asymmetric key algorithm (e.g., RSA, DHKE, ECC).

-Conduct initial research on the selected algorithms, focusing on their history, design principles, and common use cases.

-Identify known vulnerabilities and performance characteristics of each algorithm.

Deliverable:

-A brief written summary (1-2 pages) outlining the selected algorithms and a preliminary research overview. This will be later merged into the final report.

Week 9: Implementation and Initial Testing

Task:

-Implement the selected cryptographic algorithms using a programming language of choice(e.g., Python, C, Java). If existing libraries are used, ensure that the group understands the underlying implementation.

-Begin initial testing by encrypting and decrypting sample data, and measuring basic performance metrics (e.g., encryption/decryption speed).

Deliverable:

- Source code of the initial implementations.

- A short report (1-2 pages) documenting the implementation process and initial testing results. This will be later merged into the final report.

Week 10: Comprehensive Testing and Performance Analysis

Task:

- Conduct more comprehensive testing, including:

- Performance evaluation under varying conditions (e.g., different key sizes, input data sizes, input file types etc.).

- Collect data on algorithm performance characteristics. (e.g. encryption time, CPU usage, memory usage)

Deliverable:

- A detailed testing report (2-3 pages) including graphs, tables, and visualizations of the performance data. This will be later merged into the final report.

Week 11 to 13: Final Submission & Vivas

Task:

- Compile all findings into a final report, by merging all three prior sections ensuring that it is well-organized and includes all research, testing, analysis, and conclusions.

- Submit the final report and the source codes used to the link uploaded to Courseweb

- Vivas for the submitted documents will be conducted according to a schedule published on Courseweb

Deliverable:

- Final report (up to 9 pages with the cover page) with all sections integrated. Include references in IEEE format wherever necessary. (Click here to learn IEEE referencing format)

- Source code submission.

Submission Information

- The report and source code need to be uploaded as a Zip file to Course-Web.
- Rename the Report to include all IT Numbers. *E.g. IT1234567_IT7656322_IT6483839.pdf*

- Only the group leader should submit the document.

- The deadline for submission of the completed coursework will be announced during one of the lectures.

- Late submissions are **NOT** allowed, and **Plagiarism** will not be tolerated.

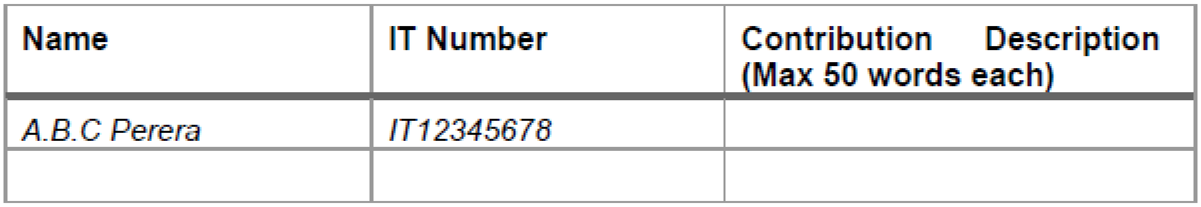
- You should bring a **printed copy** of your assignment to your viva session.

IMPORTANT

Cover page should indicate the following:

1. Selected Algorithm Names

2. A table as below:



Name	IT Number	Contribution Description (Max 50 words each)
A.B.C Perera	*IT12345678*	

Evaluation Criteria:

- **Research Quality (20%)**: Depth and accuracy of the initial research on the selected algorithms.

- **Implementation and Testing (30%)**: Correctness and completeness of the algorithm implementations and the thoroughness of the testing process.

- **Analysis (30%)**: Clarity and depth of the performance analysis, including the analysis of real-world applications.

- **Presentation and Communication (20%)**: Quality of the final report and the ability to effectively communicate findings.

Tools and Resources:

Programming Languages: Python, C, Java, or any language that supports cryptographic libraries.

Libraries and Tools: PyCrypto, OpenSSL, Crypto++, or similar cryptography-focused libraries.

Documentation: Research papers, textbooks, and online resources related to cryptographic algorithms and their evaluation.

Marking Scheme

Criteria	Excellent (80–100%)	Very Good (65–79%)	Satisfactory (50–64%)	Poor (35–49%)	Very Poor (0–34%)
1. Research Quality (20%)	Thorough, current sources; clear comparisons; risks + mitigations; flawless IEEE.	Strong, recent sources; minor gaps; clear justification; ≤2 IEEE slips.	Adequate overview; limited comparison; superficial risks; citation issues.	Sparse/outdated sources; unclear justification; major IEEE errors.	Little/incorrect research; no/uncited sources; plagiarism.
2. Implementation and Testing (30%)	Correct AES + RSA/ECC + hash; secure params; CSPRNG; reproducible tests; time/CPU/RAM; multiple trials.	Correct overall; minor issues; broad tests missing one metric; mostly reproducible.	Runs for basics; limited breadth; small keys/no auth; timing only; weak docs.	Partial; API misuse (e.g., ECB); ad-hoc tests; not reproducible.	Doesn’t run or wrong; severe crypto misuse; no tests.
3. Analysis (30%)	Clear insights; compare speed/CPU/RAM/security; variance shown; labeled graphs; limits + justified recommendations.	Solid comparisons; minor omissions; conclusions mostly supported.	Results reported; minimal interpretation; generic recommendations.	Misreads or omits evidence; weak visuals; no clear takeaways.	No analysis; contradictions.
4. Presentation & Communication (20%)	≤9 pages; clear structure; readable figures; perfect IEEE; correct packaging; confident, accurate viva.	Minor style/length issues; mostly correct IEEE; good viva.	Cluttered or inconsistent visuals; several IEEE errors; average viva.	Disorganized; unreadable visuals; missing cover info; weak viva.	Non-compliant or no viva; plagiarism.