Wilfrid Laurier University
Department of Physics and Computer Science
CP-460-Applied Cryptography
Dr. Abbas Yazdinejad

Project Proposal and Approval Form

1. Your Name/s (Team members):

2. Email Address/es:

3. Project Title:

4. Brief Project Description (Max 500 words):

5. References:
(a)
(b)
(c)
(d)

Approve by: Date:

Final Report due on 25th Nov.

Project Continuation

Students are invited to propose their own project or work in a group with no more than three members. Once a proposed project is approved, no requests to change group members or switch to individual work will be accepted. All group members will receive the same grade, so please ensure that the workload is distributed fairly and that everyone contributes equally.

If you choose to work as a team on the project, only one team member needs to submit the project form, report, and any other related materials. The project may encompass one or more of the following areas:

1. A critical review of a significant article (e.g., from journal papers or magazines).
2. An evaluation of two methods proposed in different papers.
3. Further development or analysis of an existing approach or idea.
4. A novel approach, technique, analysis, or algorithm.

Each project must include a literature review from at least one journal or magazine article. Recommended journals and magazines include:

- IEEE Transactions on Information Forensics and Security
- IEEE Transactions on Dependable and Secure Computing
- IEEE Security and Privacy
- Springer Journal of Cryptology
- ACM Transactions on Privacy and Security
- USENIX Conferences
- ACM CSS

It is advisable to consult the materials listed in the references of your selected paper to gain a comprehensive understanding of the topic of interest. Additionally, utilize the bibliographical notes and references provided in the textbook for further materials.

Sample topics may include:

- Security aspects of IoT devices or networks
- Authentication and data integrity methods in 5G or 6G networks
- Comparative analysis of stream and block ciphers
- Concepts and techniques of group-key or session key management
- Digital or crypto cash systems
- Secure web-based purchase orders
- Virtual election booths, etc.

Report Guidelines

The final report constitutes 30 percent of the final grade. The report should not exceed 10-20 pages, including figures and references. It should be neat, readable, and self-contained, written with the potential readership in mind. Every class member should be able to understand and derive benefits from the results obtained in your report. Therefore, you must include adequate references and/or background materials. Utilize tables, diagrams, graphs, figures, and excerpts of printouts to enhance the comprehension of your project by the readers.

Suggested Report Format

The following structure is recommended for your report. While adherence to this format is not mandatory, and modifications may be required based on the specifics of your project, it is imperative that you type and paginate your report. The sections suggested are as follows:

1. **Abstract**: This section should be positioned at the beginning of your report but written last. It should provide a concise summary of your project, including the purpose, methods used, main findings, and conclusions.
2. **Introduction**: This should include relevant background material and a literature review. Discuss the scope of your project and any limitations you have identified.
3. **Discussion**: This constitutes the main body of your report and should detail the methodology you employed. Be thorough in describing any figures, tables, or diagrams used, ensuring they are fully explained within the text.
4. **Results**: Present the findings of your project here, clearly and systematically.
5. **Conclusions**: Summarize the implications of your results and what they contribute to the field.
6. **Recommendations**: Offer suggestions for future work and outline any problems that remain unresolved.
7. **References**: This section is mandatory and should comply with either the American Psychological Association (APA) or IEEE citation styles. For more detailed guidelines, visit APA and IEEE Citation Styles.
8. **Appendices**: Include any supporting material that is relevant but not essential to the main text of your report.

Note on Academic Integrity: Plagiarism involves the unauthorized use or close imitation of the ideas and language of another author and representing them as one's own original work. This includes using materials from any source without proper acknowledgment. Ensure all sources are accurately cited, direct quotes are indicated with quotation marks, and paraphrasing is kept to a necessary minimum. Excessive paraphrasing without proper citation is also considered plagiarism. If you are unsure about how to properly credit sources, please consult me for guidance.

Please consider **Project Report Rubric** outlined in Table 1 to ensure your submission meets the expected criteria for organization, content, understanding, and use of references.

Table 1: Project Report Rubric

Criteria	Exceptional	Outstanding	Strong	Moderate	Insufficient
Organization	The report is structured exceptionally well, facilitating an easy understanding and seamless flow of ideas.	The report is very well organized, promoting clarity and a logical progression of ideas.	The report is organized effectively with a clear structure.	The organization of the report is adequate but may lack some clarity in the flow of ideas.	The report's organization is poor, making it difficult to follow the progression of ideas.
Content	The content is presented and argued exceptionally well; ideas are thoroughly detailed, extensively developed, and	Content is well-presented and argued; ideas are detailed, well-developed, and include most relevant specifics.	Content is reliable and solid; ideas are present and correct but lack detailed development.	Content meets basic criteria but lacks depth and detail. Required word count may not be met.	Content lacks depth and coherence, and does not meet the required word count.

	supported by specific evidence.				
Understanding	Demonstrates an exceptional understanding of the security issues, with insights that indicate a deep comprehension beyond basic knowledge.	Displays a strong grasp of the security issues, showing a clear understanding and ability to discuss them effectively.	Shows a competent understanding of the security issues, though some aspects may not be fully explored.	Understanding of the security issues is present but superficial.	Shows poor understanding of the security issues, with many concepts not addressed or misunderstood.
References	References are exceptionally well-integrated, significantly enhancing the argument. All sources are cited flawlessly according to APA or IEEE style.	References are effectively integrated and support the claims made, with only minor citation errors. All conform to APA or IEEE style.	References support the arguments but may not be seamlessly integrated into the narrative. Minor errors in APA or IEEE style citations.	References are present but poorly integrated and incorrectly cited according to APA or IEEE style.	The report lacks adequate references, and the few included are incorrectly cited according to APA or IEEE style.

Best of luck with your projects!