Detailed Project Proposal (DPP)

Student Number: 20070587

Student Name: Mahmud Hasan

Course: MSc Software Engineering with Advanced Research

Supervised by: Joseph Williams

* **Project Title**

Comparative study of cryptography algorithms and its’ applications.

* **MSc Project title (Module Code and Title)**

7COM1039-0109-2022 - Advanced Computer Science Masters Project

* **Student name and Student ID Number**

Mahmud Hasan, 20070587

* **Aim of the project**

The aim of the project will be to discuss different types of cryptographic algorithms and a comparative study between them according to real-world use examples.

* **Research question/ hypothesis**

"What are the strengths and weaknesses of different cryptographic algorithms, and how do they perform in real-world applications such as secure communication, data protection, and authentication?"

This question can be broken down into several sub-questions, such as:

1. What are the main cryptographic algorithms used today, and what are their key features and characteristics?
2. How do these algorithms compare in terms of security, speed, and efficiency?
3. What are the most common applications of cryptographic algorithms, and what are the specific requirements and constraints of these applications?
4. How do different algorithms perform in specific use cases, such as secure messaging, online transactions, or cloud storage?
5. What are the current trends and challenges in the field of cryptography, and how are they shaping the development and use of cryptographic algorithms?

Answering these questions can provide valuable insights into the strengths and limitations of cryptographic algorithms and help inform the design and implementation of secure systems and applications.

* **Objectives**

1. Evaluate the performance and security characteristics of different cryptographic algorithms: By comparing and analyzing the performance and security features of various cryptographic algorithms, researchers can determine which algorithms are suitable for particular applications.
2. Assess the usability and compatibility of cryptographic algorithms: Cryptographic algorithms can be complex and difficult to implement and integrate with other systems. A comparative study can evaluate the usability and compatibility of different cryptographic algorithms with different types of hardware and software.
3. Investigate the impact of quantum computing on current cryptographic algorithms: The development of quantum computing could have a significant impact on current cryptographic algorithms. Researchers can study the impact of quantum computing on the security of different algorithms and the development of post-quantum cryptographic algorithms.
4. Identify areas for future research: A comparative study can identify areas where further research is needed to improve the security and performance of cryptographic algorithms.
5. Provide recommendations for selecting appropriate cryptographic algorithms: Based on the research findings, a comparative study can provide recommendations for selecting the most suitable cryptographic algorithms for specific applications.

Overall, the main objective of a comparative study of cryptographic algorithms and their applications is to improve the security, performance, and usability of cryptographic systems.

* **Short description of the idea**

There will be and introduction of cryptographic algorithms following by detailed discuss of different types of Symmetric Cryptographic Algorithms and Asymmetric Cryptographic Algorithms. Performance analysis of different cryptographic algorithms according to their application.

* **Specify the plan to conduct this research**

Planning to conduct research on a comparative study of cryptographic algorithms and their applications involves several steps, including:

1. Defining the research question: The first step in conducting research is to define the research question, which in this case is to compare different cryptographic algorithms and their applications. This question should be specific and focused.
2. Literature review: Conducting a thorough literature review to identify and evaluate existing research on cryptographic algorithms is important. This will help in identifying the strengths and weaknesses of different algorithms and also help in identifying the gaps in the existing literature.
3. Data collection: Collecting data is a crucial step in any research. In this case, the data could include different types of cryptographic algorithms, their applications, and their strengths and weaknesses. The data could be collected through various sources such as academic journals, books, online resources, and industry reports.
4. Data analysis: Once the data is collected, it needs to be analyzed to identify trends, patterns, and themes. This will help in identifying the key similarities and differences between the cryptographic algorithms and their applications.
5. Interpretation and conclusion: Finally, the results of the research need to be interpreted and a conclusion drawn. This conclusion should be based on the analysis of the data and should help to answer the research question. The conclusion should also identify any limitations of the research and suggest directions for future research.
6. Writing the research report: Once the analysis is complete, the research findings should be compiled in a research report. The report should follow the standard structure of a research paper, including an introduction, literature review, methodology, results, discussion, and conclusion. Proper citation and referencing of sources using an appropriate referencing style should be included.

Citation - MNB Anwar, M Hasan, MM Hasan, JZ Loren, S.M.T Hossain. "Comparative Study of Cryptography Algorithms and Its' Applications." International Journal of Computer Networks and Communications Security 7, no. 5 (2019): 96-103.