|  |  |
| --- | --- |
| Book Name: | **Finite Abelian Groups, Elliptic Curves, Blockchain with Hashing and Graphs** |
| Manuscript Number: | **Ms\_BPR\_3842.8** |
| Title of the Manuscript: | **A Python Programming Initiative for Hash Construction Through the Example of SHA-2** |
| Type of the Article | **Book chapter** |

General guidelines for the Peer Review process:

This Book’s peer review policy states that **NO** manuscript should be rejected only on the basis of ‘**lack of Novelty’**, provided the manuscript is scientifically robust and technically sound. To know the complete guidelines for the Peer Review process, reviewers are requested to visit this link:

<https://r1.reviewerhub.org/general-editorial-policy/>

**Important Policies Regarding Peer Review**

Peer review Comments Approval Policy: <https://r1.reviewerhub.org/peer-review-comments-approval-policy/> Benefits for Reviewers: <https://r1.reviewerhub.org/book-benefits-for-reviewers>

|  |
| --- |
| **PART 1: Review Comments** |
| **Compulsory** REVISION comments | **Reviewer’s comment** | **Author’s Feedback** *(Please correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback**here)* |
| **Please write a few sentences regarding the importance of this manuscript for the scientific community. Why do you like (or dislike) this manuscript? A minimum of 3-4 sentences may be required for this part.** | This manuscript presents a valuable example of implementing the SHA-2 has algorithm in Python, which could be useful for teaching cryptography and related concepts. The step-by- step explanation of the algorithm and its implementation is commendable, as it allows readers to understand the complexities of hash construction. However, the manuscript could be enhanced by improving the clarity and organization of the code, potentially through the use of comments and more descriptive variable names. Additionally, the manuscript's impact could be increased by providing a more comprehensive discussion of the SHA-2 algorithm's security and performance aspects. Overall, this manuscript provides a solid foundation for understanding SHA-2 implementation and could serve as a good starting point for furtherresearch and development in this area. |  |
| **Is the title of the article suitable?****(If not please suggest an alternative title)** | The title "A PYTHON PROGRAMMING INITIATIVE FOR HASH CONSTRUCTIONTHROUGH THE EXAMPLE OF SHA-2" is suitable and informative as it accurately reflects the content of the manuscript, which focuses on constructing a hash using Python programming with the SHA-2 algorithm as an example. |  |

|  |  |  |
| --- | --- | --- |
| **Is the abstract of the article comprehensive? Do you suggest the addition (or deletion) of some points in this section? Please write your suggestions here.** | The abstract of the article is not comprehensive. It lacks specific details about the SHA-2 algorithm, its implementation in Python, and the potential applications of this work.Suggestions for additions:* Briefly mention the SHA-2 algorithm and its importance in cryptography.
* Highlight the key features of the Python implementation, such as the step-by-step explanation and the use of functions for specific operations.
* Emphasize the educational value of this work for understanding hash construction and cryptography concepts.
* Briefly discuss the potential applications of this implementation, such as in security systems or data integrity verification.
 |  |
| **Are subsections and structure of the manuscript appropriate?** | The subsections and structure of the manuscript are generally appropriate but could benefit from some improvements. Below is the breakdown:**Strengths:*** **Clear progression:** The manuscript follows a logical flow from introducing SHA-2 to explaining its Python implementation.
* **Well-defined sections:** The use of sections and subsections helps organize the content, making it easier for readers to follow.

**Areas for improvement:*** **More informative headings:** Some headings could be more descriptive. For example, "4 SHA-2 Implementation" could be "4 Python Implementation of SHA-2".
* **Further subdivide long sections:** Section 3, "Preprocessing," is quite lengthy and covers multiple distinct steps. Subdividing it further could improve readability.
* **Reorganize the code:** The Python code presentation could be improved by grouping related functions together.
* **Explicit conclusion:** The manuscript ends abruptly after the code example. Adding a concluding section to summarize the work and its implications would be beneficial.

**Specific suggestions:*** Consider adding a subsection specifically on the SHA-2 algorithm's background and significance in cryptography.
* Reorganize the Python code to group functions by their purpose (e.g., binary conversion functions, constant definitions, rotation functions, compression functions).
* Add a concluding section to summarize the work, reiterate its educational value, and suggest potential applications or future research directions.
 |  |
| **Please write a few sentences regarding the scientific correctness of this manuscript. Why do you think that****this manuscript is scientifically robust and technically sound? A minimum of 3-4 sentences may be required** | * The manuscript could benefit from some additional explanation of the Python code. For example, the authors could provide more details on the purpose of each function and how the different functions work together.
 |  |

|  |  |  |
| --- | --- | --- |
| **for this part.** | * The manuscript could also be improved by providing some additional examples of how the program can be used. For example, the authors could show how to use the program to hash different types of messages.
* The authors should also consider adding some error handling to the Python code. This would help to ensure that the program is robust and can handle unexpected input.

Despite these minor issues, the manuscript is a valuable contribution to the field of cryptography. It provides a clear and concise explanation of the SHA-2 algorithm and a working Python implementation. I believe that this manuscript would be of interest to anyone who wants to learn more about SHA-2 or who needs to implement it in Python.In addition to the above comments, I would also like to suggest the following improvements:* The authors could consider adding a section on the security of the SHA-2 algorithm. This would help to provide readers with a better understanding of the strengths and weaknesses of the algorithm.
* The authors could also consider adding a section on the performance of the Python implementation. This would help to give readers an idea of how efficient the implementation is.
 |  |
| **Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form.****-** |  |  |

|  |  |  |
| --- | --- | --- |
| Minor REVISION comments**Is the language/English quality of the article suitable for scholarly communications?** | The manuscript is well-written and informative, with a clear and concise explanation of the SHA-2 algorithm and its Python implementation. However, it could benefit from a few improvements:* The Python code could be explained in more detail, clarifying the purpose of each function and how they work together.
* Additional examples of the program's usage, such as hashing different message types, would be helpful.
* Adding error handling to the Python code would improve its robustness and ability to handle unexpected input.

Despite these minor issues, the manuscript makes a valuable contribution to cryptography by providing a clear explanation and working implementation of the SHA-2 algorithm. |  |
| **Optional/General** comments | The manuscript is well-written and informative. The authors have done a good job of explaining the SHA-2 algorithm and providing a clear and concise Python implementation. However, there are a few minor issues that need to be addressed.A few minor issues:* The manuscript could benefit from some additional explanation of the Python code. For example, the authors could provide more details on the purpose of each function and how the different functions work together.
* The manuscript could also be improved by providing some additional examples of how the program can be used. For example, the authors could show how to use the program to hash different types of messages.
* The authors should also consider adding some error handling to the Python code. This would help to ensure that the program is robust and can handle unexpected input.

This manuscript presents a valuable example of implementing the SHA-2 hash algorithm in Python, which could be useful for teaching cryptography and related concepts. The step-by- step explanation of the algorithm and its implementation is commendable, as it allows readers to understand the complexities of hash construction. However, the manuscript could be enhanced by improving the clarity and organization of the code, potentially through the use of comments and more descriptive variable names. Additionally, the manuscript's impact could be increased by providing a more comprehensive discussion of the SHA-2 algorithm's security and performance aspects. Overall, this manuscript provides a solid foundation for understanding SHA-2 implementation and could serve as a good starting point for further research and development in this area. |  |
| **PART 2:**  |
|  | **Reviewer’s comment** | **Author’s comment** *(if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)* |
| **Are there ethical issues in this manuscript?**  | *(If yes, Kindly please write down the ethical issues here in details)* |  |

|  |
| --- |
| **Reviewer Details:** |
| Name: |  |
| Department, University & Country |  |

|  |
| --- |
| **Editorial Comments (This section is reserved for the comments from book editorial office and editors):** |
|  | Author’s Feedback |
|  |  |

**Reviewer Details:**

**This information is mandatory to prepare the Reviewer Certificate properly. Certificate preparation will not be possible if incomplete information is received.**

|  |  |
| --- | --- |
| Name of the Reviewer | Sravanthi Dontu |
| Department of Reviewer | Department of Information Technology |
| University or Institution of Reviewer | University of The Cumberlands |
| Country of Reviewer | United States of America |
| Position: (Professor/lecturer, etc.) of Reviewer | IT Professional |
| Email ID of Reviewer | Sravanthi.dontu13@gmail.comsravanthi.dontu13@gmail.com |
| WhatsApp Number of Reviewer (Optional) |  |
| 5-8 Keywords regarding expertise of Reviewer |  |