**Data Encryption Standard (DES): Operation Modes Implementation**

Submitted in partial fulfilment of the **CAPSTONE PROJECT** in VIRTUALIZATION TECHNOLOGY, which is a part of

**Integrated M. Tech. in Cybersecurity**

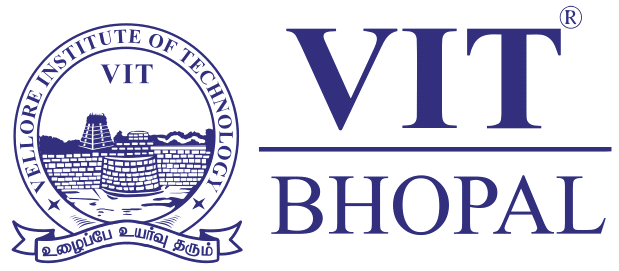
By

**Nihal Awasthi**

**22MEI10055**

Submitted to

**Dr. Hemraj S. Lamkuche**



School of Computing Science and Engineering,

VIT Bhopal University, Madhya Pradesh

India

*October 2023*

**Motivation**

For all the heading levels, their spacing, fonts, numbering, nested level, etc. have been set. In chapter one, at each heading level, corresponding heading number in styles is given at the first instance of use. Similarly, for captions (tables, figures, etc.) everything has been set, including their alignment, spacing, etc. So, from the Styles on the home tab in the ribbon in MS Word, select the appropriate style required for your text.

Table of contents, tables, figures, etc. have been automated but will be useful only *if you remember to use automated captions while labelling the same*. For this, use insert caption tab under references tab on the MS word ribbon

Thanks!

**Capstone Project Approval**

This is to certify that the Integrated M. Tech. Capstone Project report titled **“Data Encryption Standard (DES): Operation Modes Implementation”** by **Nihal Awasthi** (*22MEI10055*) is approved for the degree of **Integrated M. Tech. in Cybersecurity**.

**Date****: 17/10/2023** **Dr. Hemraj S. Lamkuche**

**Place**: VIT Bhopal (Course Coordinator)

**Declaration**

I declare that this written submission represents my ideas in my own words and where other’s ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honestly and integrity and have not misrepresented or fabricated or falsified any ideas, data, facts or sources in my submission. I understand that any violation of the above will be cause of disciplinary action by the institute and evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

**Date**: 17/10/2023  **Nihal Awasthi**

**Place**: VIT Bhopal  **22MEI10055**

**Abstract**

Data Encryption Standard (DES) is a widely recognized symmetric-key algorithm for the encryption of electronic data. The security and reliability of this algorithm have made it a cornerstone in the field of cryptography. Understanding its operation modes is crucial to comprehend its application in securing sensitive information. This paper presents an in-depth exploration of the various operation modes used in DES, including Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) modes. We delve into the intricacies of these modes, analyzing their strengths and weaknesses in different data protection scenarios.

Furthermore, this paper provides an overview of the DES algorithm, discussing its key components such as the initial and final permutations, key generation, round function, and permutation functions. The implementation details for each operation mode are examined, highlighting the specific steps involved in the encryption and decryption processes. Practical insights and examples elucidate the application of each mode, illustrating how DES ensures data confidentiality, integrity, and authenticity.

By critically evaluating the implementation aspects of various operation modes, this research aims to provide a comprehensive understanding of DES, enabling stakeholders to make informed decisions regarding data security strategies. The analysis presented in this paper contributes to the existing literature on data encryption techniques, emphasizing the importance of robust cryptographic mechanisms in safeguarding sensitive information in the digital era.

Table of Content

Contents

[Motivation i](#_Toc46518328)

[Capstone Project Approval iii](#_Toc46518329)

[Declaration v](#_Toc46518330)

[Abstract vii](#_Toc46518331)

[Table of Contents ix](#_Toc46518332)

[List of Figures x](#_Toc46518333)

[List of Tables x](#_Toc46518334)

[List of Graphs x](#_Toc46518335)

[List of Appendices x](#_Toc46518336)

[Nomenclature xiii](#_Toc46518337)

[Chapter 1 Title, style Heading 1 1](#_Toc46518338)

[1.1 Title Case Level One heading, style Heading 2 1](#_Toc46518339)

[1.1.1 Lower case level two heading, style Heading 3 1](#_Toc46518340)

[1.2 Structure of Report 2](#_Toc46518341)

[Chapter 2 Chapter Two 5](#_Toc46518342)

[2.1 Is the Scientific Project? 5](#_Toc46518343)

[2.2 Inserting Footnotes 5](#_Toc46518344)

[2.2.1 Use of technical language 5](#_Toc46518345)

[2.2.2 Referencing 6](#_Toc46518346)

[Chapter 3 Chapter Three 7](#_Toc46518347)

[3.1 One 7](#_Toc46518348)

[3.1.1 One point one 7](#_Toc46518349)

[Chapter 4 Title 9](#_Toc46518350)

[Chapter 5 Conclusion 11](#_Toc46518351)

[Appendix 13](#_Toc46518352)

[References 15](#_Toc46518353)

[Acknowledgements 17](#_Toc46518354)

* **List of Figures**

Figure 1.1: Caption 2

* **List of Tables**

Table 1.1: Caption 2

* **List of Graphs**

Graph 31 1

* **List of Appendices**

Appendix I 1

Appendix II 1

**Nomenclature**

* **Title: Data Encryption Standard (DES): Operation Modes Implementation**
* **Author: Nihal Awasthi**
* **Registration Number: 22MEI10055**
* **Institution: VIT Bhopal university**
* **Course: MAT2009**
* **Professor: Dr. Hemraj S. Lamkuche**
* **Date of Submission: [Submission Date]**

**Chapter 1**

**Title, Style Heading 1**

* **Title Case Level One Heading, Style - Heading 2**

Tell what you are going to tell in the introduction. Then in tell what you want to tell. Then sum up what you told and connect to what will be next (tell what you will be telling after this). Follow this advice in every chapter, every section as well and you will create a wonderful document. Though, you can skip it in favour of brevity and if you already have a nice clarity.

* **Lower case level two heading, style - Heading 3**

*Hypothesis non fingo – Issac Newton in Principia, 1713*

I have not as yet been able to discover the reason for these properties of gravity from phenomena, and I do not feign hypotheses. For whatever is not deduced from the phenomena must be called a hypothesis; and hypotheses, whether metaphysical or physical, or based on occult qualities, or mechanical, have no place in experimental philosophy. In this philosophy particular propositions are inferred from the phenomena, and afterwards rendered general by induction.

[*http://en.wikipedia.org/wiki/Hypotheses\_non\_fingo*](http://en.wikipedia.org/wiki/Hypotheses_non_fingo)

* *Level three heading, style Heading 4*

*Table .: Automated Caption using Insert caption in Reference tab*

|  |  |
| --- | --- |
| **Heading row** |  |
| As per your preference, remove space after paragraph for table to compress the lines used in the table. |  |
|  |  |
|  |  |

*Figure .: Automated Caption*

* **Structure of Report**

Chapter 1 Introduction – contains background, motivation, broad societal concern to main objective, context of problem, Structure of Report

Chapter 2 Literature review – review of literature including background, basic info about the sector/ topic being researched, methods being used, geographies being explored, any other topical literature. This can also propose literature/ research gaps.

Chapter 3 – Research Methodology – contains short note the methodology of the research – Quant/ qual, mixed, ontology, epistemology. Followed by research questions, objectives, sub research questions, tasks, sub tasks, methods for each SRQ, etc. as preferred by your guide. Continue with scope of your study and important boundaries that you have set at the beginning.

Chapter 4 – Results – based on your methods, the outputs of your tasks go here. Arranged sequentially as per your RQs, this can be broken into more chapters as needed and appropriately titled.

Chapter 5 – Discussions – discusses results and findings using existing literature, your insights from other sources, views. Here you try to triangulate/ vet your results.

Chapter 6 – Conclusions – includes summary of your results, records how you have addressed all the research questions and completed your work, gives limitations of the current study, has a section on future work.

Details of what should go in each section is described in the guidelines and by your guides as well, so follow them if any conflict with what i have proposed.

**Chapter Two**

**Is the Scientific Project?**

This article explains the logic of scientific process and how it should proceed; also, how a scientific communication should be written actually, which is different than what you are supposed to be writing right now

* **Inserting Footnotes**

Follow these steps

* Take cursor after the word where you want to footnote marker to be displayed
* Click on References, the fifth tab (after File, Home, Insert and Page Layout)
* Click on Insert footnote
* Now type your footnote at the bottom of the page where the cursor goes automatically. You can easily edit this as per your need, later on.
* **Use of technical language**

<https://eng.kuleuven.be/prev/english/education/reporting/language-style>

<http://www.sussex.ac.uk/ei/internal/forstudents/engineeringdesign/studyguides/techreportwriting>

both these are supporting informations, if they clash with what VITB guidelines or your guides say, ignore them. But these are good, standard rules to a great extent

* **Referencing**

Try to reference every comment you make that is not your own. Using APA style,

<https://apastyle.apa.org/>

you can practically cite any source, including twitter, youtube, etc. it is up to you to confirm veracity, quality of the source.

Based on your discipline, you might use IEEE, Chicago and other styles. Most of these can be automated within word or using citations manager such as Mendeley.

**Chapter Three**

* **One**
* **One point one**

*Graph*

* **Title**
* **Conclusion**

Once the report is done, it’s time to take the enquiry further.

Will VITB ever consider using other fonts than the Times New Roman in report submissions? Does anyone actually check if all the details of styles are followed in the documents submitted? Where can we access past reports, search through them, like we search for journals?

* **Appendix**

*Appendix*

Number one

*Appendix*

Number two

* **References**
* **Acknowledgements**

If I thought anyone cared, if I thought anyone would even be reading this, I'd probably make an effort to keep up appearances until the last possible moment. But no one does, and no one will. So I can pretty much say exactly what I think.

Oh, yes, the *acknowledgements.* I think not. I did it. I did it all, by myself.

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | ABC | | Bhopal | | September 4, 2023 | |