A black background with a black square

Description automatically generated with medium confidence**Assessment cover**

**STUDENTS, PLEASE COPY THIS PAGE AND USE AS THE COVER PAGE FOR YOUR FINAL SUBMISSION**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Module No: |  | | | Module title: |  | |
| Degree Programme : | |  | | | | |
| Project title : | |  | | | | |
| Supervisor : | |  | | | | |
| Due date and time**:** | |  | | | | |
| Estimated total time to be spent on assignment: | | | | | | **90 hours per student** |
| **Student No:** | | | **Student Name:** | | | |
|  | | |  | | | |

**Statement of Compliance *(please tick to sign)***

I declare that the work submitted is my own and that the work I submit is fully in accordance with the University regulations regarding assessments *(*[*www.brookes.ac.uk/uniregulations/current*](http://www.brookes.ac.uk/uniregulations/current)*)*

**Regulations governing the deposit and use of Oxford Brookes University Projects and Dissertations**

Copies of projects/dissertations, submitted in fulfilment of Modular Programme requirements and achieving marks of 60% or above, shall normally be kept by the Library.

**Statement of Permission *(please tick to sign)***

|  |  |
| --- | --- |
|  | | agree that this dissertation and associated deliverables may be available for reading and photocopying in accordance with the Regulations governing use of the Library. |

**Use of AI Tools**

You are required to use this [form](https://docs.google.com/forms/d/e/1FAIpQLSfjGiLTf7NEGMVeaZe62ufUxUs7kmw6HayzYTNKKioz_D3G2Q/viewform) to declare which AI tools you have used and how you have used them. Please complete the form and attach it to your submission as an Appendix, if you have used such tools.

**LEARNING OUTCOMES**

|  |  |
| --- | --- |
| **On successful completion of this module, students will be able to achieve the module following learning outcomes (LOs):** | |
| 1 | Create, design, manage, plan, carry out, and evaluate a project involving the solution of a practical problem set in an appropriate social and economic context, taking into account other relevant factors such as risk |
| 2 | Apply practical and analytical skills acquired in the programme to the investigation of a substantial topic |
| 3 | Apply the scientific method and report findings using accepted formalisms |
| 4 | Identify and utilise trustworthy information sources, such as the ACM Digital Library to develop a coherent understanding of issues in the domain |
| 5 | Demonstrate the ability to carry out a substantial piece of work independently and critically evaluate the student’s achievements and their own personal development |
| 6 | Use appropriate technologies such as online libraries and databases to find, critically evaluate and utilise both non-specialist and technical information pertinent to the project |
| 7 | Demonstrate an awareness of and work in a manner guided by the legal, professional, ethical, security and social issues relevant to the IT and telecommunications industry |

|  |  |
| --- | --- |
| **Engineering Council AHEP4 LOs assessed (from S1 2022-23):** | |
| **B3** | Select and apply appropriate computational and analytical techniques to model broadly-defined problems, recognising the limitations of the techniques employed |
| **B4** | Select and evaluate technical literature and other sources of information to address broadly-defined problems |
| **B5** | Design solutions for broadly-defined problems that meet a combination of societal, user, business and customer needs as appropriate. This will involve consideration of applicable health & safety, diversity, inclusion, cultural, societal, environmental and commercial matters, codes of practice and industry standards |
| **B6** | Apply an integrated or systems approach to the solution of broadly-defined problems |
| **B7** | Evaluate the environmental and societal impact of solutions to broadly-defined problems |
| **B8** | Identify and analyse ethical concerns and make reasoned ethical choices informed by professional codes of conduct |
| **B9** | Use a risk management process to identify, evaluate and mitigate risks (the effects of uncertainty) associated with a particular project or activity |
| **B10** | Adopt a holistic and proportionate approach to the mitigation of security risks |
| **B13** | Select and apply appropriate materials, equipment, engineering technologies and processes |
| **B15** | Apply knowledge of engineering management principles, commercial context, project management and relevant legal matters |
| **B17** | Communicate effectively with technical and non-technical audiences |

**FORMATIVE FEEDBACK OPPORTUNITIES**

|  |
| --- |
| **Your supervisor will give you the following formative feedback:**   * Weekly, during project supervision meetings * Written feedback on Proposal (See Appendix A) * Written feedback on Progress Report (See Appendix B) * Feedback on presentation draft |

**SUMMATIVE FEEDBACK DELIVERABLES**

|  |  |
| --- | --- |
| **Deliverable description and instructions** | **Weighting out of 100%** |
| Presentation (see Appendix C) comprising:   1. presentation of software, with video URL 2. project slides 3. summary poster (i.e. the final project slide) | **10%** |
| Final Report (see Appendix D) comprising:   1. written dissertation 2. software artefact URL link to source code | **90%** |

# **A Study of Effectiveness of Historic and Modern Encryption Methods**

## **Table of Contents**

## **Glossary - 5**

## **Glossary**

AES – Advanced Encryption Standard, the internets “default” encryption algorithm

Asymmetric – Two separate keys are used, on for encryption and one for decryption

Ciphertext – The result of encrypting the plaintext with an algorithm

DES – Data Encryption Standard, an outdated algorithm, widely replaced by AES

Encryption Ratio – The difference in size between the plaintext and the ciphertext

Plaintext – The message, or data, to be encrypted

Public-Key – A version of asymmetric key systems where one key is broadcast at the start of communication, and one is kept private

RSA – Rivest-Shamir-Adleman, a public-key modern encryption algorithm

Symmetric – The same key is used to encrypt and decrypt

Triple DES – A variant of DES where 2 or 3 keys are used in a sequence of subsequent encryptions and decryptions

## **Abstract**

This report focuses on a gap I found in research based on what encryption algorithm is most suited for a particular task, encrypting text or images. Therefore, I have designed my own version of 10 different encryption algorithms; 5 historic and 5 modern and tested them against the two tasks. I have implemented them using Python 3.12 and included a basic GUI for users to recreate my results and test their own theories. By the end of this report, I will have a detailed report on the performance of these separate algorithms for each separate task, scored on a scale I have come up with, including but not limited to Encryption Speed, Decryption Speed and Encryption Ratio. Needs Addition

## **Acknowledgements**

I would like to thank Mr. David Lightfoot for assisting me throughout this process.

## **Introduction**

### **Background**

Very frequently, when I am creating something that requires security, I have wondered what particular algorithm would be best for the use case I require, be it encrypting text to send over a network connection, or simply encrypting a file to store. This is why I have decided to complete this study, as a means to be a easy access for others who require the same information.

### **Aim**

This study will aim to judge how effective different encryption methods are for different purposes. I will be testing 10 separate algorithms on both text and image encryption. These will be 5 historic algorithms and 5 modern algorithms as detailed below. For the image encryption, instead of modifying the algorithms themselves, I will be converting the binary data stored inside the PNG files into text based on a fixed alphabet that I have created, similar to the base64 alphabet but with the + and / symbols replaced.

### **Objectives**

My objectives are as follows:

* To develop a scoring system to judge effectiveness of algorithms
* To research and develop 10 separate encryption algorithms
* To develop software for testing the encryption methods using Python’s inbuilt tkinter module
* To use this to score the algorithms on both image and text encryption
* To bring this data together into an easy-to-read format for other developers to use

### **Product Overview**

My end product is this report that will bring together all the data I have collected together for other developers to use when they need it. The final algorithms I have chosen will be: Caesar Shift, Substitution Cipher, Vigenère Cipher, Rail-Fence Cipher, Enigma, RSA, DES, Triple DES, Blowfish and AES. The scoring system will be based on encryption and decryption speeds, key size, encryption ratio and key generation time. I will also include an additional analysis of each algorithm based on security and how easy it is to crack.

## **Background Review**

I found a pre-existing study around this idea *(Panda, 2016, pp.278-284)* that

evaluates various algorithms using Encryption time, Decryption Time and

Throughput. This differs to mine as I intend to not only use audio encryption, but I will

also be judging the algorithms differently. They have a good range of modern

encryption algorithms, though no historic ones and the data they gathered is very

clear and easy to read. I can use this data to double check my code in my testing

stage using the same inputs they did.

Another paper I found *(Yadav and Majare, 2016, pp. 70-73)* evaluates them very differently (Throughput, Key Size, Encryptionand Decryption Speed and Time, Encryption Ratio and Level of Security Issues)however they do not encrypt images or audio. I believe this is a much more robustway of judging algorithms than just purely speed and I will use this as a basis forhow I judge my algorithms. A very recent paper I found *(Paradesi Priyanka et al.,*

*2022, pp.295-300)* does things differently. Rather than scoring them they have

compared them using the standard speed, security and power consumption most of

the others use, however they also compare the against each other with their age,

algorithm type (symmetric/asymmetric) and inherent vulnerabilities (brute-force, side-

channel attack and oracle attack). I like this approach as you can truly tell an

algorithm’s strength and security with age. An older paper *(Singh, G. and Supriya,*

*2013)* has a similar approach to this however they include Triple DES as well as

DES, AES and RSA. Interestingly they found that AES was more secure than DES

as well as 3DES with both *(Paradesi Priyanka et al., 2022, pp.295-300)* and *(Singh,*

*G. and Supriya, 2013)* ranking RSA as the least secure. I will be interested to see

how my research will differ. Another approach by (Padmavathi, B. and Ranjitha

Kumari, S., 2013) is to rank AES, DES and RSA based purely on time and buffer

size. I do not believe this is enough criteria to accurately rank each algorithm against

each other. Papers *(Paradesi Priyanka et al., 2022, pp.295-300)* through to

*(Padmavathi, B. and Ranjitha Kumari, S., 2013)* only test algorithms on text or binary

files, albeit of various sizes. There is very limited data on audio encryption however I

was able to find a paper *(Rizvi, S.A.M, Hussain, S.Z. and Wadhwa, N., 2011, pp.76-*

*79)* that tests both AES and TwoFish against various factors using text, image and

audio files. This is a very in-depth study of these 2 algorithms and the data shows

that TwoFish is almost equal to AES in everything except audio encryption where it

surpasses it. This is probably due to the fact that AES was almost TwoFish *(Schneier.com, 2019)* where it was only beaten by what was previously known as “Rijndael Block Cipher Family” referring to a selection of ciphers which are now know as AES-128, AES-192, AES-256. *(Dworkin, 2023)*.

## **Methodology**

### **Approach**

To develop my project, I will be using an modified agile model, using weekly progress updates and designed each individual part of the software slowly, testing as I go, ensuring it works as intended. For requirement gathering, I used a brainstorming method where I write down functional and non-functional requirements and develop on those ideas. As I test my software whilst developing, I will update a mirror document of the brainstorming with progress updates and completion dates.

### **Technology**

I will not require much technology for this project, just access to python for the coding, GitHub for version management and Microsoft Word/Google Docs for documentation.

### **Version Management Plan**

For version management, I will be using a GitHub repository that I will be making regular commits to. This can be found at: <https://github.com/ryanbutbored/ComputingProject>

## **Results**

fssfegsgfg

## **Bibliography**

1. Panda, M. (2016) ‘Performance Analysis of Encryption Algorithms for

Security’ 2016 International Conference on Signal Processing,

Communication, Power and Embedded System (SCOPES), Paralakhemundi,

India, pp. 278-284, DOI: 10.1109/SCOPES.2016.7955835.

1. G. Yadav and A. Majare (2016) ‘A Comparative Study of Performance Analysis of Various Encryption Algorithms’ International Journal on Recent and Innovation Trends in Computing and Communication, 5 (3) pp. 70-73 Available at

[https://ijritcc.org/download/conferences/ICEMTE\_2017/Track\_2\_(EXTC)/1487](https://ijritcc.org/download/conferences/ICEMTE_2017/Track_2_(EXTC)/1487794878_22-02-2017.pdf)

[794878\_22-02-2017.pdf](https://ijritcc.org/download/conferences/ICEMTE_2017/Track_2_(EXTC)/1487794878_22-02-2017.pdf)

Accessed: 09/03/2024

1. M. Paradesi Priyanka et al., (2022) "A Comparative Review between Modern

Encryption Algorithms viz. DES, AES, and RSA," 2022 International

Conference on Computational Intelligence and Sustainable Engineering

Solutions (CISES), Greater Noida, India, pp. 295-300, DOI:

10.1109/CISES54857.2022.9844393.

1. Singh, G. and Supriya, (2013) ‘A Study of Encryption Algorithms (RSA, DES,

3DES and AES) for Information Security’ International Journal of Computer

Applications, 67(19). Available at:

<https://research.ijcaonline.org/volume67/number19/pxc3887224.pdf>

Accessed: 09/03/2024

1. Padmavathi, B. and Ranjitha Kumari, S. (2013) ‘ A Survey on Performance

Analysis of DES, AES and RSA Algorithm along with LSB Substitution

Technique’ International Journal of Science and Research, 2(4).

Accessed at:

<https://www.ijsr.net/archive/v2i4/IJSRON120134.pdf>

Accessed: 09/03/2024

1. Rizvi, S.A.M, Hussain, S.Z. and Wadhwa, N. (2011) ‘Performance Analysis of

AES and TwoFish Encryption Schemes‘ 2011 International Conference on

Communication Systems and Network Technologies, Katra, India, pp. 76-79.

DOI: 10.1109/CSNT.2011.160

1. Schneier.com. (2019). Schneier on Security: Twofish. [online]

Available at: <https://www.schneier.com/academic/twofish/>.

Accessed: 10/03/2024

1. Dworkin, M.J. (2023). Advanced Encryption Standard (AES). NIST. [online] Available at: <https://www.nist.gov/publications/advanced-encryption-standard-aes-0>.

Accessed: 10/03/2024