**TOPIC OF THESIS**

****

**By**

**NAME**

**CMS # 11111**

**Supervised by  
Dr.**

**Department of Cybersecurity and Data Science,**

**RIPHAH INSTITUTE OF SYSTEMS EGINEERING,**

**FACULITY OF COMPUTING,**

**RIPHAH INTERNATIONAL UNIVERSITY,**

**ISLAMABAD, PAKISTAN**

**SRING 2018**

**TOPIC OF THESIS**

****

**By**

**NAME**

**CMS # 11111**

**Supervised**

**By**

**Dr. Muhammad Yousaf**

A dissertation submitted in the partial fulfillment of the requirements for the degree of

**MASTER OF SCIENCE**

**IN**

**INFORMATION SECURITY**

**Department of Cyber security and Data Science,**

**RIPHAH INSTITUTE OF SYSTEMS EGINEERING,**

**Faculty of Computing,**

**RIPHAH INTERNATIONAL UNIVERSITY,**

**ISLAMABAD, PAKISTAN**

**RIPHAH INTERNATIONAL UNIVERSITY, ISLAMABAD**

**APPROVAL SHEET**

**SUBMISSION OF HIGHER RESEARCH DEGREE DISSERTATION/THESIS**

|  |  |
| --- | --- |
| Candidate’s Name: |  |
| CMS Number: |  |
| Program Title: |  |
| Department/ Faculty: | Riphah Institute of Systems Engineering, |
| Dissertation Title: |  |

I hereby certify that the above candidate’s work, including the Dissertation/thesis, has been completed to my satisfaction and that the Dissertation/thesis is in a format and of an editorial standard recognized by the department/faculty as appropriate for examination. The Dissertation/thesis has been checked through Turnitin for plagiarism (test report attached).

Supervisor: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The undersigned certify that:

1. The candidate presented at a pre-completion seminar, an overview and synthesis of major findings of the Dissertation/thesis, and that the research is of a standard and extent appropriate for submission as a Dissertation/thesis.

2. I have checked the candidate’s Dissertation/thesis and its scope, format, and editorial standards are recognized by the department/ faculty as appropriate.

3. The plagiarism check has been performed. Report is attached.

|  |  |
| --- | --- |
| Head of Department: |  |
| Dean of Faculty: |  |

**Declaration**

I certify that the research work presented in this dissertation/thesis is to the best of my knowledge my own. All sources used, and any help received in the preparation of this dissertation/thesis have been acknowledged. I hereby declare that I have not submitted this material, either in whole or in part, for any other degree at this or any other institution.

I understand the zero tolerance policy of HEC and Riphah International University Islamabad towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/ cited.

I undertake if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS IS degree, the University reserves the right to withdraw/ revoke my MS IS degree and that HEC and the university has the right to publish my name on the HEC/ university website on which names of students are placed who submitted plagiarized thesis.

*Signature……………….*

**ACCEPTANCE CERTIFICATE**

Mapping Introvert and Extrovert From Twitter Data Using NLP

**By**

**Sana Tabasum**

A dissertation submitted in the partial fulfillment of the requirements for the degree of Master of Science in Data Science

We accept this dissertation as conforming to the required standard.

**Examination Committee:**

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Supervisor,**  Dr.Adeel Zafar,  Associate Professor,  Riphah Institute Of Systems Engineering,  Riphah International University,  Islamabad | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Co. Supervisor,** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **External Examiner,**  Dr. Hassan Mujtaba | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Dr. Muhammad Yousaf,**  Director,  Riphah Institute Of Systems Engineering,  Riphah International University,  Islamabad |

**DEPARTMENT OF CYBER SECURITY AND DATA SCIENCE, FACULTY OF COMPUTING, RIPHAH INTERNATIONAL UNIVERSITY, ISLAMABAD, PAKISTAN**

**SPRING 2022**

**Dedication**

This thesis is dedicated to my family specially my mom, my father, my fiance and friends. Thank you for your prayers and support and please continue this in future as well.

**Acknowledgements**

First, I would like to thank Almighty ALLAH

Rashid Ali

**List of Tables**

[Table 1.1 Statistical Hypothesis Testing – Errors **Error! Bookmark not defined.**](#_Toc536106182)

[Table 2.1 Randomness Testing Batteries and Corresponding Tests **Error! Bookmark not defined.**](#_Toc536106183)

[Table 2.2 A Dynamic Look-up Table **Error! Bookmark not defined.**](#_Toc536106184)

[Table 2.3 Summary Table of Related work 8](#_Toc536106185)

[Table 4.1 Length Required for Statistical Tests of NIST **Error! Bookmark not defined.**](#_Toc536106186)

[Table 4.2 P Value Results Generated via NIST **Error! Bookmark not defined.**](#_Toc536106187)

[Table 4.3 P Value Results Generated via NIST for Non‐Overlapping Template **Error! Bookmark not defined.**](#_Toc536106188)

[Table 4.4 P Value Results Generated via NIST for Serial **Error! Bookmark not defined.**](#_Toc536106189)

[Table 4.5 P Value Results Generated via NIST for Cusum **Error! Bookmark not defined.**](#_Toc536106190)

[Table 4.6 P Value Results Generated via NIST for Random Excursions **Error! Bookmark not defined.**](#_Toc536106191)

[Table 4.7 P Value Results Generated via NIST for Random Excursion Variant **Error! Bookmark not defined.**](#_Toc536106192)

**List of Figures**

[Figure 2.2.1 Default view of NIST statistical test suite **Error! Bookmark not defined.**](#_Toc536102981)

[Figure 3.1 System Diagram How an Improved Statistical Test Suit Works **Error! Bookmark not defined.**](#_Toc536102982)

[Figure 3.2 Architectural Illustration of Strategies for Statistical Analysis of Cryptographic algorithms 11](#_Toc536102983)

[Figure 3.3 Overview of an improved statistical test suite **Error! Bookmark not defined.**](#_Toc536102984)

[Figure 4.1 Data Input methodology 1 **Error! Bookmark not defined.**](#_Toc536102985)

[Figure 4.2 Data Input methodology 2 **Error! Bookmark not defined.**](#_Toc536102986)

[Figure 4.3 Data Output inform of Bit Stream **Error! Bookmark not defined.**](#_Toc536102987)

[Figure 4.4 Data Statistical Tests Output **Error! Bookmark not defined.**](#_Toc536102988)

[Figure 4.5 Results Interpretation on Graph **Error! Bookmark not defined.**](#_Toc536102989)

# ABSTRACT

Information Security is one of the biggest challenges of today’s world and without

**Table of Contents**

[ABSTRACT xi](#_Toc536111271)

[Chapter 1: Introduction 4](#_Toc536111272)

[1.1 Introduction 6](#_Toc536111273)

[1.2 What is Randomness **Error! Bookmark not defined.**](#_Toc536111274)

[1.3 Random Number Generators (RNGs) and Pseudorandom Number Generators (PRNGs) **Error! Bookmark not defined.**](#_Toc536111275)

[1.4 Testing Theory **Error! Bookmark not defined.**](#_Toc536111276)

[1.5 Considerations for Randomness, Unpredictability and Testing **Error! Bookmark not defined.**](#_Toc536111277)

[1.6 Problem Statement **Error! Bookmark not defined.**](#_Toc536111278)

[1.7 Significance of Work and Potential Benefit **Error! Bookmark not defined.**](#_Toc536111279)

[Summary **Error! Bookmark not defined.**](#_Toc536111280)

[Chapter 2 7](#_Toc536111281)

[Literature Survey 7](#_Toc536111282)

[2.1 Related Work / Literature Survey 8](#_Toc536111283)

[2.2 NIST Statistical Test Suit **Error! Bookmark not defined.**](#_Toc536111284)

[2.2.1 Frequency (Monbiot’s) Test **Error! Bookmark not defined.**](#_Toc536111285)

[2.2.2 Frequency within a Block Test **Error! Bookmark not defined.**](#_Toc536111286)

[2.2.3 Runs Test **Error! Bookmark not defined.**](#_Toc536111287)

[2.2.4 Longest Run of Ones in a Block Test **Error! Bookmark not defined.**](#_Toc536111288)

[2.2.5 Binary Matrix Rank Test **Error! Bookmark not defined.**](#_Toc536111289)

[2.2.6 Discrete Fourier Transform (Spectral) Test **Error! Bookmark not defined.**](#_Toc536111290)

[2.2.7 Non-overlapping Template Matching Test **Error! Bookmark not defined.**](#_Toc536111291)

[2.2.8 Overlapping Template Matching Test **Error! Bookmark not defined.**](#_Toc536111292)

[2.2.9 Maurer’s “Universal Statistical” Test **Error! Bookmark not defined.**](#_Toc536111293)

[2.2.10 Linear Complexity Test **Error! Bookmark not defined.**](#_Toc536111294)

[2.2.11 Serial Test **Error! Bookmark not defined.**](#_Toc536111295)

[2.2.12 Approximate Entropy Test **Error! Bookmark not defined.**](#_Toc536111296)

[2.2.13 Cusum Test **Error! Bookmark not defined.**](#_Toc536111297)

[2.2.14 Random Excursions Test **Error! Bookmark not defined.**](#_Toc536111298)

[2.2.15 Random Excursions Variant Test **Error! Bookmark not defined.**](#_Toc536111299)

[2.3 User’s Guide **Error! Bookmark not defined.**](#_Toc536111300)

[2.4 Dieharder **Error! Bookmark not defined.**](#_Toc536111301)

[2.5 TestU01 **Error! Bookmark not defined.**](#_Toc536111302)

[2.6 Randomness Failures **Error! Bookmark not defined.**](#_Toc536111303)

[2.7 Limitations of Existing Techniques 8](#_Toc536111304)

[2.7.1 SP800\_22\_tests **Error! Bookmark not defined.**](#_Toc536111305)

[2.7.2 NIST sts-2.1.1 statistical test suite **Error! Bookmark not defined.**](#_Toc536111306)

[2.7.3 Python 2.6 by Ilja **Error! Bookmark not defined.**](#_Toc536111307)

[2.7.4 R4nd0m **Error! Bookmark not defined.**](#_Toc536111308)

[Summary 9](#_Toc536111309)

[Chapter 3 10](#_Toc536111310)

[Proposed Solution and Methodology 10](#_Toc536111311)

[3.1 Methodology and Proposed Solution 11](#_Toc536111312)

[3.2 User Friendly Interface **Error! Bookmark not defined.**](#_Toc536111313)

[3.3 Bit Convertor **Error! Bookmark not defined.**](#_Toc536111314)

[3.4 Result interpretation **Error! Bookmark not defined.**](#_Toc536111315)

[3.5 Performance **Error! Bookmark not defined.**](#_Toc536111316)

[3.6 System Diagram **Error! Bookmark not defined.**](#_Toc536111317)

[3.7 Strategies for the Statistical Analysis of Cryptographic Algorithms **Error! Bookmark not defined.**](#_Toc536111318)

[3.7.1 Select Cryptographic Algorithm **Error! Bookmark not defined.**](#_Toc536111319)

[3.7.2 Generate a Binary Sequence **Error! Bookmark not defined.**](#_Toc536111320)

[3.7.3 Execute Statistical Tests **Error! Bookmark not defined.**](#_Toc536111321)

[3.7.4 Examine P Value **Error! Bookmark not defined.**](#_Toc536111322)

[3.7.5 Assessment: Pass/Fail **Error! Bookmark not defined.**](#_Toc536111323)

[3.8 Methodology **Error! Bookmark not defined.**](#_Toc536111324)

[3.8.1 Python **Error! Bookmark not defined.**](#_Toc536111325)

[3.8.2 Flask **Error! Bookmark not defined.**](#_Toc536111326)

[3.8.3 Advance Encryption Standard (AES) Module **Error! Bookmark not defined.**](#_Toc536111327)

[3.8.4 NIST\_STS Module **Error! Bookmark not defined.**](#_Toc536111328)

[Summary 12](#_Toc536111329)

[Chapter 4 13](#_Toc536111330)

[Implementation and Results 13](#_Toc536111331)

[4.1 Implementation and Results 14](#_Toc536111332)

[4.2 Data Input **Error! Bookmark not defined.**](#_Toc536111333)

[4.3 Parameter Adjustment **Error! Bookmark not defined.**](#_Toc536111334)

[4.4 Data Output **Error! Bookmark not defined.**](#_Toc536111335)

[4.5 Statistical test to Evaluate Cryptographic Algorithm **Error! Bookmark not defined.**](#_Toc536111336)

[4.6 Output of Statistical Tests **Error! Bookmark not defined.**](#_Toc536111337)

[4.7 Result interpretation on Graph **Error! Bookmark not defined.**](#_Toc536111338)

[4.8 Results and Discussions **Error! Bookmark not defined.**](#_Toc536111339)

[Summary 15](#_Toc536111340)

[Chapter 5 19](#_Toc536111341)

[Conclusion 19](#_Toc536111342)

[5.1 Conclusion 20](#_Toc536111343)

[References 21](#_Toc536111344)

# 

**ABBREVIATIONS**

A

Activity Dependent Appliances - ADA

Advanced Metering Infrastructure - AMI

Annual Growth Rate - AGR

Arti\_cial Intelligence - AI

B

Battery Energy Storage System

# Chapter 1 Introduction

## Problem Area

## Problem Statement

## Research Questions

## Research Objectives

## Significance of work and potential benefits

## Summary

Modern world faces lot of challenges and one of major challenge amongst them is information security. Information security is the field of defending information from

# 

# Chapter 2 Literature Survey

## Related Work / Literature Survey

In cryptographic applications based on some algorithm like AES or a block cipher, there are three main algorithms which are encryption, decryption, and key schedule algorithm. Ristenpart and Yilek have studied several other randomness attacks, where adversary can repeat, predict, or choose the randomness.

## Limitations of Existing Techniques

Known weakness of the existing approach is the complexity of the system that user face while testing randomness of the ciphertext produced by different cryptographic applications.

1. in this case it required more time in executing all tests for different samples of data. Hence it is very hard to practice this software in case of errors and exceptions for real time usage.

Table 1.1 Summary Table of Related work

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Features | User Friendly | Configuration complexity | Accuracy | Open source | Support for Hex |
| NIST STS |  |  |  |  |  |
| SP800\_22\_tests |  |  |  |  |  |
| sts2.1.1 statistical tests |  |  |  |  |  |
| Python 2.6 by Ilja |  |  |  |  |  |
| R4nd0m |  |  |  |  |  |
| TestU01 |  |  | N/A |  |  |
| Diehard |  |  | N/A |  |  |
| ENT |  | N/A | N/A |  |  |
| Crypt-XS |  | N/A | N/A |  |  |
| Improved STS |  |  |  |  |  |

As shown in Table 2.3 all the existing technologies is lacking User friendly interface, Also, they do not provide a method to be used for

## Summary

This chapter introduces different statistical test suites that are used for randomness testing to evaluate cryptographic algorithms.

# 

# Chapter 3 Proposed Solution and Methodology

## Methodology and Proposed Solution

This research is focused on improving current NIST statistical suite.

Figure 0.1 Architectural Illustration of Strategies for Statistical Analysis of Cryptographic algorithms

## Summary

In this chapter proposed solution and Methodology is explained in detail.

# 

# Chapter 4 Deployment and Implementation

## Implementation

Today’s encryption algorithms are static in nature, repeating processes over and over

## Summary

In this chapter, comparative analysis of two result sets of p values against same sample data is presented.

# Chapter 5 Results and Analysis

## Results

Today’s encryption algorithms are static in nature, repeating processes over and over

## Summary

In this chapter, comparative analysis of two result sets of p values against same sample data is presented.

# Chapter 6 Conclusion and Future Work

## Conclusion

An Improved statistical test suite for cryptographic algorithms is proposed in this research paper

# References

|  |  |
| --- | --- |
| [1] | Patil, Priyadarshini, Prashant Narayankar, D. G. Narayan, and S. Md Meena., "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish.," *Procedia Computer Science 78,* pp. 617-624, (2016). |
| [2] | Rukhin, Andrew, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications.," *Booz-Allen and Hamilton Inc Mclean Va,* 2001. |
| [3] | B. D. McCullough, "A review of TESTU01," *Journal of Applied Econometrics 21, no. 5,* pp. 677-682, 2006. |
| [4] | Alani, Mohammed M., "Testing randomness in ciphertext of block-ciphers using DieHard tests.," *Int. J. Comput. Sci. Netw. Secur 10, no. 4,* pp. 53-57, 2010. |
| [5] | W. J. ENT., "A pseudo random number sequence test program," *http://www.fourmilab.ch/random,* 1998. |
| [6] | Caelli, William., "Crypt x package documentation," *Information Security Research Centre and School of Mathematics, Queensland University of Technology,* 1992. |
| [7] | MARTON, Kinga, and Alin SUCIU, "On the interpretation of results from the NIST statistical test suite," *SCIENCE AND TECHNOLOGY 18 , no. 1 ,* pp. 18-32, 2015. |
| [8] | Li, Liang, "Testing several types of random number generator.," *The Florida State University,* 2012. |
| [9] | Afzal, Shazia, Umer Waqas, Mubeen Akhtar Mir, and Muhammad Yousaf, "STATISTICAL ANALYSIS OF KEY SCHEDULE ALGORITHMS OF DIFFERENT BLOCK CIPHERS.," *Science International 27, no. 3,* 2015. |
| [10] | Salameh, Jamal N. Bani, "A New Technique for Sub-Key Generation in Block Ciphers," *World Applied Sciences Journal 19, no. 11 ,* pp. 1630-1639, 2012. |
| [11] | Zaman, J. K. M., and Ranjan Ghosh, "A review study of NIST Statistical Test Suite: Development of an indigenous computer package.," *arXiv preprint arXiv:1208.5740,* 2012. |
| [12] | Demirhan, Haydar, and Nihan Bitirim, "Statistical testing of cryptographic randomness.," *Journal of Statisticians: Statistics and Actuarial Sciences 9, no. 1 ,* pp. 1-11, 2016. |
| [13] | M. ". Ukrop, "Randomness analysis in authenticated encryption systems.," *PhD diss., Masarykova univerzita, Fakulta informatiky,* 2016. |
| [14] | Bellare, Mihir, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham, and Scott Yilek, "Hedged public-key encryption: How to protect against bad randomness.," *International Conference on the Theory and Application of Cryptology and Information Security Springer, Berlin, Heidelberg,* pp. 232-249, 2009. |
| [15] | Yilek, Scott, "Resettable public-key encryption: How to encrypt on a virtual machine Cryptographers," *Track at the RSA Conference, pp. 41-56. Springer, Berlin, Heidelberg,* 2010. |
| [16] | D. Johnsto, "sp800\_22\_tests," *https://github.com/dj-on-github/sp800\_22\_tests,* Visited 24-12-2018. |
| [17] | StuardGordonReid, "R4nd0m," *https://gist.github.com/StuartGordonReid,* Visited 20-12-2018. |
| [18] | Daemen, Joan, and Vincent Rijmen, "AES proposal: Rijndael," 1999. |