UNIVERSITI TEKNOLOGI MARA

STATISTICAL ANALYSIS ON ENHANCED 3D-AES BLOCK CIPHER CRYPTOGRAPHIC ALGORITHM

NOR AZEALA BINTI MOHD YUSOF

MSc

September 2021

AUTHOR'S DECLARATION

I declare that the work in this thesis was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the results of my own work, unless otherwise indicated or acknowledged as referenced work. This thesis has not been submitted to any other academic institution or non-academic institution for any degree or qualification.

I, hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

Name of Student	:	Nor Azeala binti Mohd Yusof
Student I.D. No.	:	2015439374
Programme	:	Master of Science (Computer Science) – CS750
Faculty	:	Computer and Mathematical Sciences
Thesis Title	:	Statistical Analysis on Enhanced 3D-AES Block Cipher Cryptographic Algorithm
Signature of Student	:	……..
Date	:	September 2021

ABSTRACT

Randomness test is one of the measurement techniques which have been taken into consideration in the evaluation of the minimum security requirement of the block cipher algorithm. A non-random block cipher seems to be vulnerable to any type of attack. Many algorithms such as AES, LED, KTANTAN, KATAN, L-Block, SIMON, SPECK, RECTANGLE, and GRAIN-128 have performed randomness test using NIST Statistical Test Suite. Therefore, this research aims to analyse the randomness of 3D-AES, a local SPN-based block cipher algorithm. Specifically, the randomness test is performed using the NIST Statistical Test Suite which consists of 15 statistical tests. The output data sequences are generated from seven different data categories. Unfortunately, the failed test results for Cipher Block Chaining Mode (CBCM), Strict Key Avalanche (SKA), High Density Key (HDK), and Random Plaintext Random Key (RPRK) data categories indicate that 3D-AES produced non-random output binary sequences. The major failure is on the SKA data category which is used to evaluate the avalanche effect. On this basis, the enhancement on 3D-AES is proposed to achieve the ability to generate a random number and the modified version of 3D-AES named Enhanced 3D-AES. Two new functions, *ConfuseK* and *ConfuseP* have been injected into the 3D-AES. *ConfuseK* is a process of XORing the key element with its corresponding position number, whereas *ConfuseP* is a process of XORing the plaintext with its corresponding position number. These two new functions are based on the confusion method proposed by Shannon's theory since 1945. The randomness of Enhanced 3D-AES then is re-evaluated and it has passed all 15 statistical tests for all seven data categories. These research findings portray the effectiveness of the modification that has been done towards the initial version of 3D-AES. It can be concluded that Enhanced 3D-AES meets the standard security requirements for block cipher design. It is strongly suggested to implement Enhanced 3D-AES in software applications to secure data transmission.

ACKNOWLEDGEMENT

At this moment of accomplishment, I am greatly indebted to my supervisor, Assoc. Prof. Dr. Suriyani Ariffin, who accepted me as her M.Sc. student and offered me her mentorship, motherly love, and care. This work would not have been possible without her guidance and involvement, her support and encouragement from the start of the project till date. Under her guidance, I successfully overcome many difficulties and learned a lot. For all these, I sincerely thank her from bottom of my heart and will be truly indebted to her throughout my lifetime.

No research is possible without infrastructure and requisite material and resources. For this, I extend thanks to Hazlin Abdul Rani, Head of Cryptography Development Department, CyberSecurity Malaysia, for giving me permission to use the company's equipment and part timely carry out my research even during working hours.

It's my fortune to gratefully acknowledge the support of my colleagues in the Cryptography Development Department for providing me their valuable guidance, suggestions, and support throughout my research project work.

Finally, I acknowledge the people who mean a lot to me, my parents, for showing faith in me and giving me the liberty to choose what I desired. I salute you all for the selfless love, care, pain, and sacrifice you did to shape my life. I would never be able to pay back the love and affection showered upon by my parents.

I owe thanks to a very special person, my husband, Zulfikar Syukridosi for his continued and unfailing love, support, and understanding during the pursuit of my M.Sc. degree that made the completion of the thesis possible. You were around at times I thought that it is impossible to continue, you helped me to keep things in perspective. I greatly value his contribution and deeply appreciate his belief in me. I appreciate my babies, my little girls, Nur Ayra Syifaa and Nur Ayna Syifaa for abiding my ignorance and the patience they showed during my thesis writing. Words would never say how grateful I am to both of you.

I thank Allah the Almighty for giving me the strength and patience to work through all these years for successfully completing this long and challenging journey.

Alhamdulillah.

TABLE OF CONTENTS