CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

Research methodology is the guidance in conducting research that directs researchers towards the goal of the research. A proper planning and root cause analysis of the research scope helps researchers to link the objectives of the research, processes required in achieving the objectives, and output that can be expected from the processes. This chapter highlights the overview of the methodology used to conduct the research. The research processes are described in detail which explained the objectives and the expected output of this research. Materials and equipment used to execute the research are also mentioned. In addition, brief information on the methods used for data collection is addressed in the chapter.

3.2 Research Method

A proper methodology in designing research is required to ensure that the objectives are met and the outputs are produced as expected. In conducting this research, the activities are divided into three phases including Phase 1 (Analysis), Phase 2 (Development), and Phase 3 (Evaluation). Figure 3.1 displays the flow diagram of the processes conducted in this research.

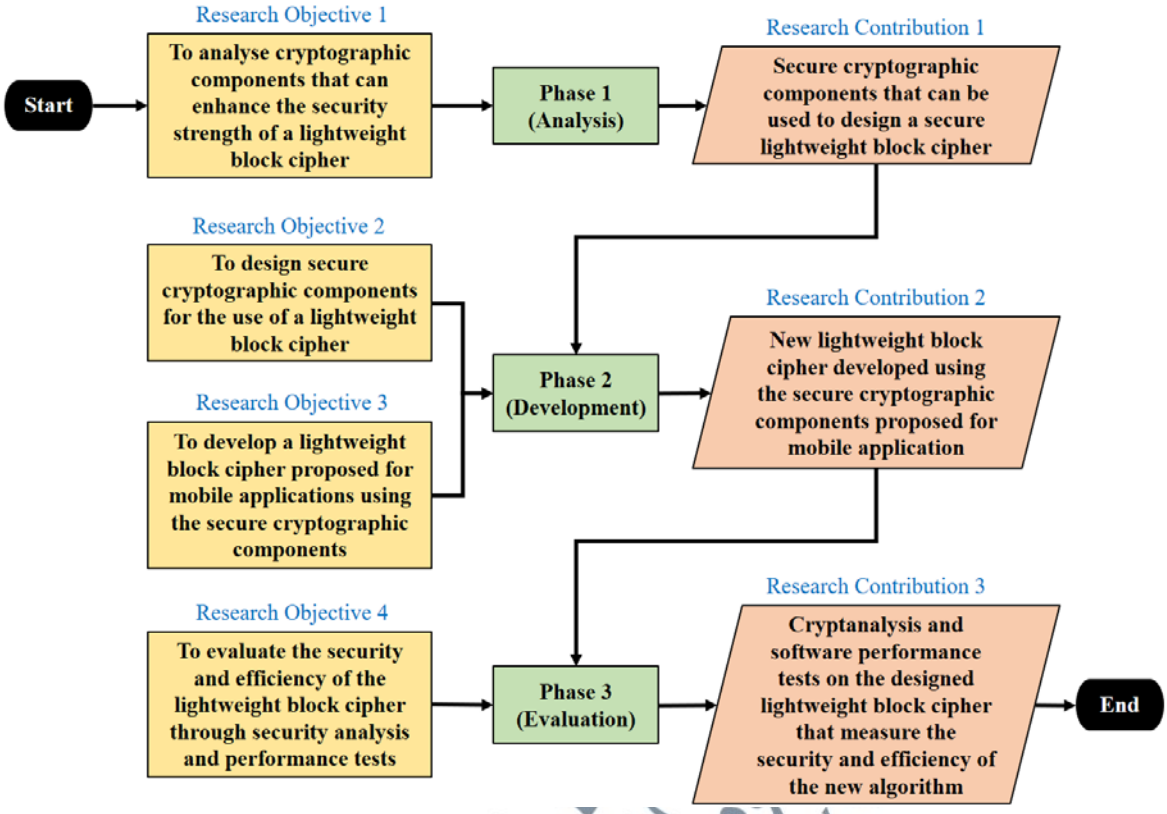

Figure 3.1: Flow of Research Process

For better viewing of the methodology implemented in this research, Table 3.1 presents the mapping of the research question, research objective, research process, and research contribution. This mapping is very important to ensure that every research question is answered with the specific research objective through a planned research process in order to produce significant research contributions in solving the identified research problem.

Table 3.1: Research Methodology Mapping

Phase	Research Question	Research Objective	Research Process	Research Contribution
Phase 1 (Analysis)	1) How does lightweight block cipher become the security solution for resource-constrained devices?	1) To analyse cryptographic components that can enhance the security strength of a lightweight block cipher	1) Define the basic requirements in developing a lightweight block cipher	1) Secure cryptographic components that can be used to design a secure lightweight block cipher
	2) How does the strength of lightweight block cipher being determined in accordance with cryptographic standards?		2) Define the security evaluation criteria for lightweight block cipher	
	3) How do cryptographic components give impact to the security of a lightweight block cipher?		3) Analysis of cryptographic components that can enhance the security strength of a lightweight block cipher	
Phase 2 (Development)	4) How does the 3D rotation method improve the strength of cryptographic algorithm design?	2) To design secure cryptographic components for the use of a lightweight block cipher	4) Formulation of the 3D rotation function	2) New lightweight block cipher developed using the secure cryptographic components proposed for mobile applications
	5) How does the encryption algorithm solve issues highlighted in security product?	3) To develop a lightweight block cipher proposed for mobile applications using the secure cryptographic components	5) Development of the key schedule algorithm	
			6) Development of the encryption algorithm	
Phase 3 (Evaluation)	6) How do encryption algorithms being distinguished in terms of security strength and software performance?	4) To evaluate the security and efficiency of the lightweight block cipher through cryptanalysis and performance test	7) Experimental setup for the security and efficiency evaluations	3) Cryptanalysis and software performance tests on the designed lightweight block cipher that measures the security and efficiency of the new algorithm
	7) How does cryptographic design influence the security of an encryption algorithm?		8) Conduct cryptanalysis on the lightweight block cipher	
	8) How does cryptographic design influence the software performance of an encryption algorithm?		9) Conduct software performance tests on the lightweight block cipher	

3.2.1 Phase 1 (Analysis)

Phase 1 is the initial step in conducting the research as shown in Figure 3.2. This is a very crucial stage that leads the direction of the research. *Research Objective 1* is to analyse cryptographic components that can enhance the security strength of a lightweight block cipher. In order to achieve the aim of the research, three processes are required to be carried out. The first process is to define the basic requirements in developing a lightweight block cipher. Next, define the security evaluation criteria for the lightweight block cipher. Lastly, analysis of cryptographic components that can enhance the security strength of a lightweight block cipher. Research processes of Phase 1 were conducted in Chapter 4 where the secure cryptographic components were analysed from the existing lightweight block ciphers, thus producing *Research Contribution 1* which is the identification of secure cryptographic components that can be used to design a secure lightweight block cipher.

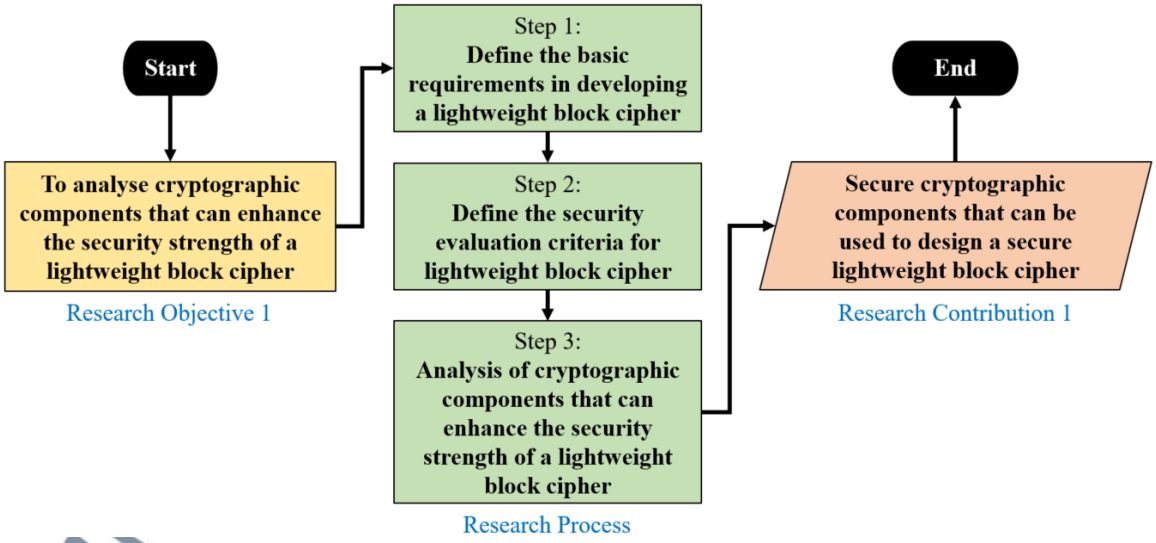

Figure 3.2: Analysis Process

3.2.2 Phase 2 (Development)

Phase 2 consists of the steps that are required to achieve *Research Objective 2* which is to design secure cryptographic components for the use of a lightweight block cipher as shown in Figure 3.3. Apart from that, Phase 2 aims to fulfil *Research Objective 3* which is to develop a lightweight block cipher proposed for mobile applications using the secure cryptographic components. Phase 2 adopted and enhanced the secure cryptographic components of the lightweight block cipher identified in Phase 1 to develop a new algorithm. The secure cryptographic components are important to ensure that the design meets the condition of a secure algorithm. Three processes are required in the development phase. The first process is the formulation of the 3D rotation function. Next is the development of the key schedule algorithm. Finally, the development of the encryption algorithm is discussed in Chapter 6. Research processes of Phase 2 produced *Research Contribution 2* which is the development of a new lightweight block cipher developed using the secure cryptographic components proposed for mobile applications.

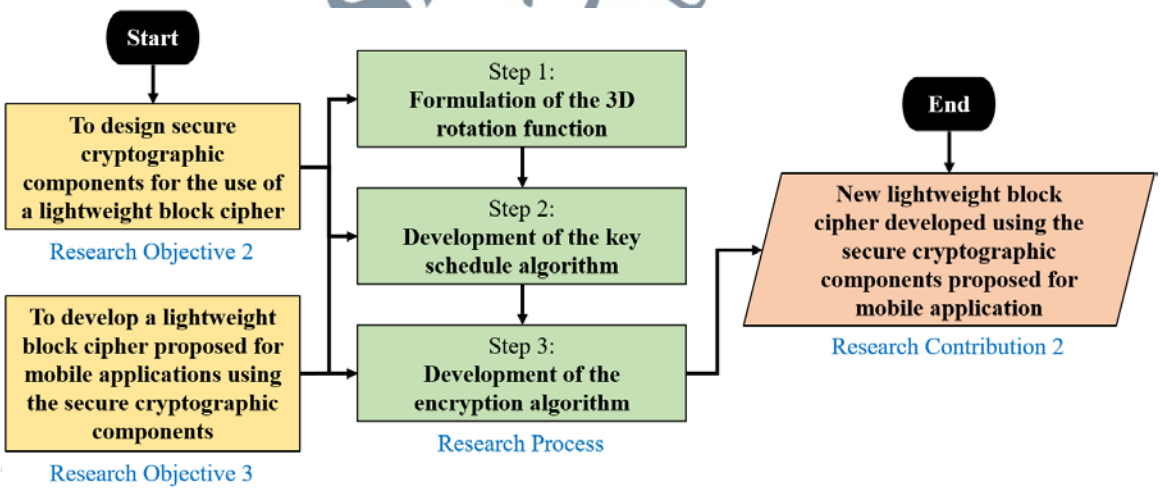

Figure 3.3: Development Process

3.2.3 Phase 3 (Evaluation)

Phase 3 contains the methods to evaluate the new lightweight algorithm as shown in Figure 3.4. *Research Objective 4* is to evaluate the security and efficiency of the lightweight block cipher through cryptanalysis and performance test. Three processes are required to evaluate the security and efficiency of the new algorithm. The first process is the experimental setup for the security and efficiency evaluation. Next, the second process is to conduct cryptanalysis on the lightweight block cipher that is discussed in Chapter 7. Lastly, the third process is to conduct software performance tests on the lightweight block cipher that are discussed in Chapter 8. Research processes of Phase 3 produced *Research Contribution 3* which is the cryptanalysis and software performance tests on the designed lightweight block cipher that measures the security and efficiency of the new algorithm.

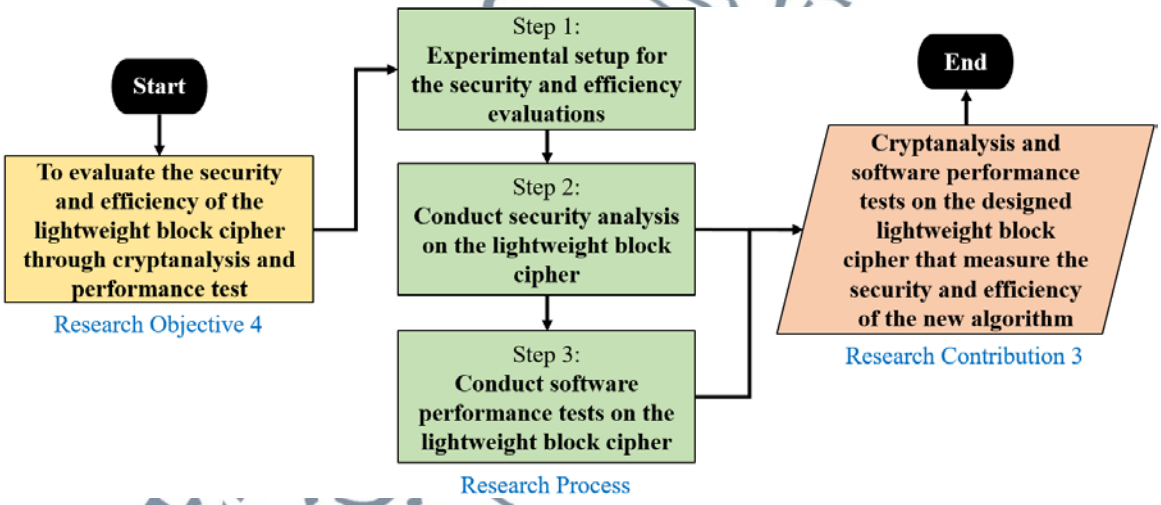

Figure 3.4: Evaluation Process

3.3 Experimental Setup

An experimental setup is a scientific experiment where the evaluation procedures are performed towards the lightweight block cipher. There are three types of security experiments that are carried out; avalanche effect, randomness tests, and cryptanalysis attacks. The avalanche effect tests can analyse the non-linearity characteristics of a lightweight block cipher, the randomness tests are able to evaluate the randomness characteristics of the ciphertext, and the cryptanalysis attacks can be used to assess the security strength of a cryptographic algorithm against attacks. On top of that, software performance tests are conducted that include execution speed and throughput evaluations. The tools used in conducting the research are listed in Table 3.2.

Table 3.2: Research Tool

Tool	Specification
Hardware (Computer)	Processor: Intel(R) Core(TM) i7-6820HQ CPU @ 2.70 GHz
	Memory: 8.00 GB RAM
	System: 64-bit Operating System
Programming Software	Microsoft Visual Studio 2008 (9.0.21022.8 RTM)
Application Development Software	Android Studio (Bumblebee 2021.1.1)
Analysis Software	NIST Statistical Test Suite (Sts-2.1.2)
	Microsoft Excel 2016
Writing Software	Microsoft Word 2016
	Mendeley Desktop (1.19.6)
	REF-N-WRITE
	XMind (7.5)
	Notepad++
	Microsoft PowerPoint 2016

Since there are three types of security experiments to assess the security strength of the proposed lightweight block cipher, different sample data sets are used in the assessment. The sample data sets can be obtained from APPENDIX J to ensure that the experiments can be replicated using the same input and the results can be compared to the other lightweight block ciphers.

3.3.1 Avalanche Effect Tests

Avalanche effect measures the robustness of a cryptographic algorithm by observing changes to the output caused by modifications in the input. The avalanche effect consists of three tests which are correlation, bit error rate, and key sensitivity tests as shown in Figure 3.5. This experiment requires the generation of random keys and random plaintexts to be used as the input for the algorithm. The random plaintext and ciphertext generated from the block cipher are used in all three tests. Results from the tests are analysed to obtain the security strength of the new lightweight block cipher.

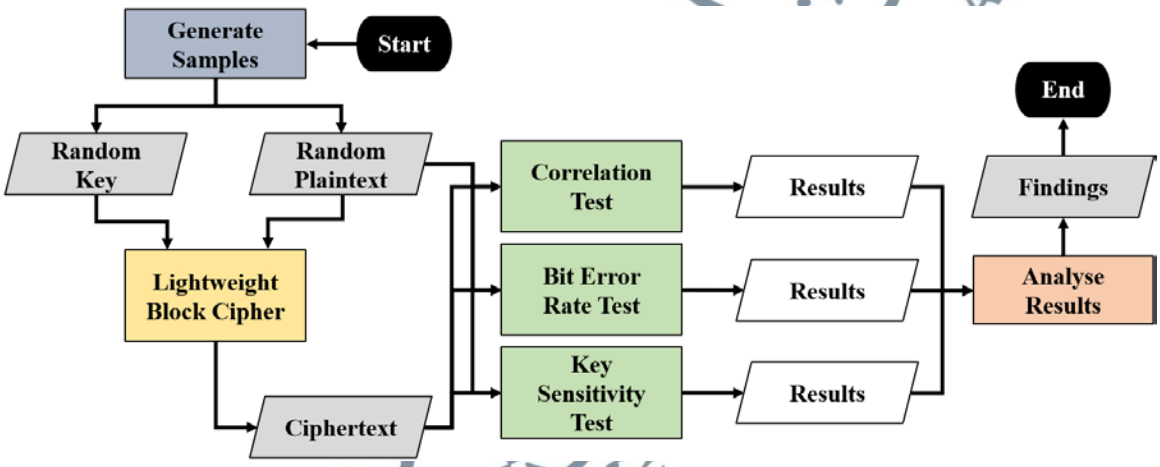

Figure 3.5: Avalanche Effect Tests Process

3.3.2 Randomness Tests

Randomness tests are conducted on the lightweight block cipher by implementing the NIST Statistical Test Suite which consists of 15 statistical tests as shown in Figure 3.6. In order to determine the randomness of ciphertext produced by the algorithm, the test suite requires a large sequence of bits. For the block cipher, nine different data categories are used to generate the ciphertext as suggested by the NIST (Soto, 1999). The data categories consist of Strict Key Avalanche (SKA), Strict Plaintext Avalanche (SPA), Plaintext/Ciphertext Correlation (PCC), Cipher Block Chaining Mode (CBCM), Random Plaintext/Random Key (RPRK), Low Density Key (LDK), High Density Key (HDK), Low Density Plaintext (LDP), and High Density Plaintext (HDP). The ciphertexts produced by the data categories are used as the input for the test suite. Results in the form of *p*-values are analysed to determine the randomness of the new lightweight block cipher.

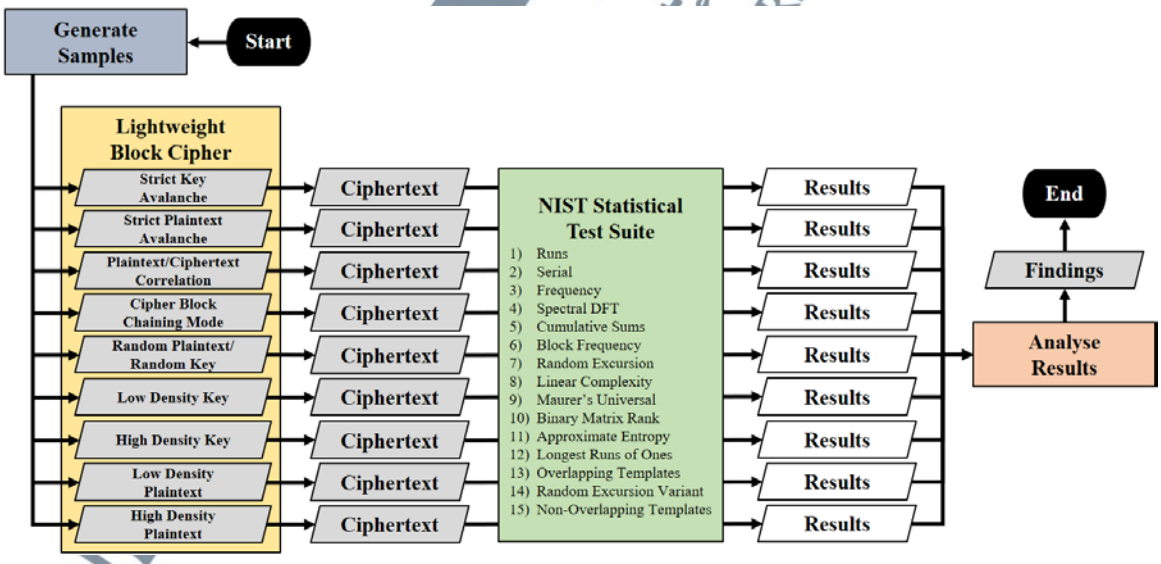

Figure 3.6: Randomness Tests Process

3.3.3 Cryptanalysis Attacks

Cryptanalysis attacks are methods to distinguish a cryptosystem from a random function. In order to ensure that confidentiality is robustly provided by the new algorithm, it is essential to investigate the security of the lightweight block cipher against a variety of attacks. This research is focusing on the two most common cryptanalysis attacks that are differential cryptanalysis and linear cryptanalysis due to their broad implementations in research publications and cryptographic projects. For experimental execution, a defined plaintext is required and the ciphertext generated from the lightweight block cipher is used as the input for the differential cryptanalysis and linear cryptanalysis as shown in Figure 3.7. Results obtained from the experiments are analysed to determine the security strength of the new lightweight block cipher.

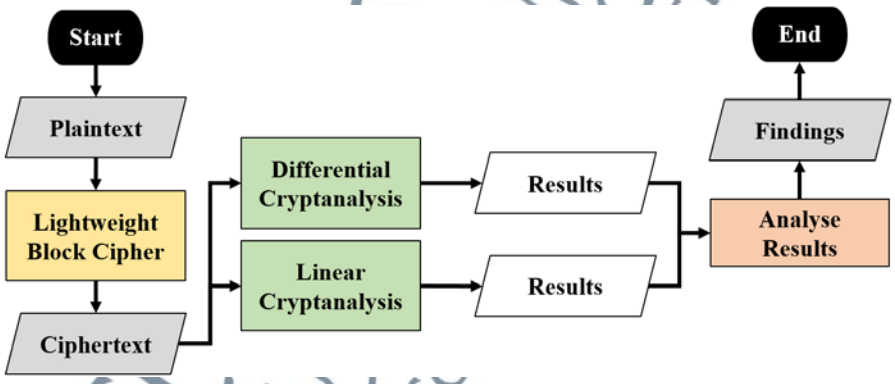

Figure 3.7: Cryptanalysis Process

3.3.4 Software Performance Tests

Software performance tests observe the time required to execute an encryption process in order to generate a ciphertext block. In addition, throughput tests evaluate the impact of cipher design on the lightweight block cipher throughput. In this experiment, the expected performance of the lightweight block cipher should be better as compared to the conventional algorithms due to its design simplicity. The expected results are important to address the issues raised in the implementation of conventional algorithms in security products. Random keys and random plaintexts are required to be generated as the input for the algorithm in conducting the performance tests as shown in Figure 3.8. The execution speed of the algorithm are recorded and the ciphertext throughputs are computed. Results obtained from the experiments are analysed to determine the efficiency of the new lightweight block cipher.

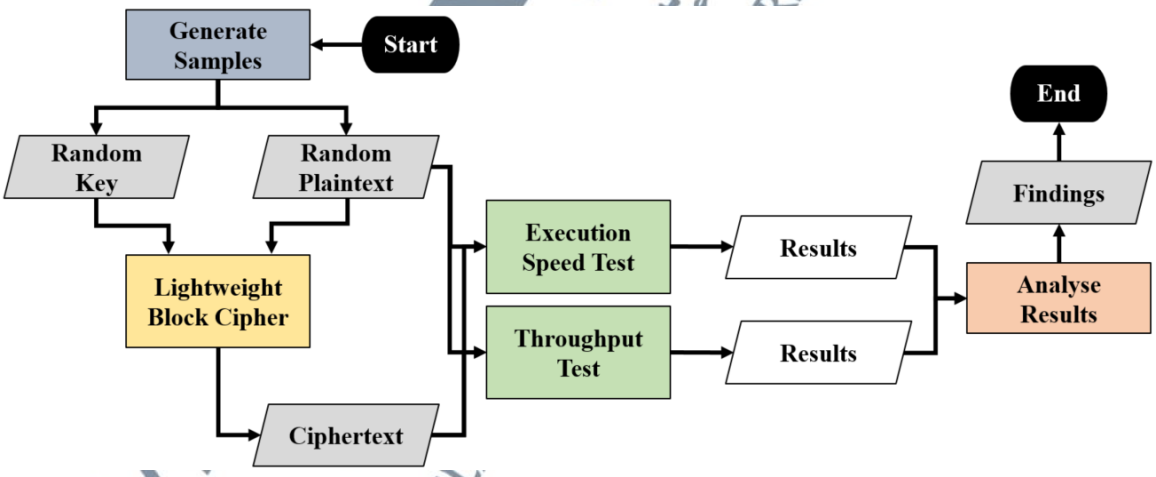

Figure 3.8: Software Performance Tests Process

3.4 Chapter Summary

This research identified three phases that are required in achieving the objectives. Phase 1 aims to analyse the secure cryptographic components of lightweight block ciphers. The secure cryptographic components that have been analysed in Chapter 4 were used for the development of a new lightweight block cipher in Phase 2 of the research.

In Phase 2, the target is to develop a new lightweight block cipher using the 3D rotation function. A proper literature review and understanding of the structure, design, and requirements of lightweight cryptography were needed before the development of the algorithm. The new algorithm is able to solve security issues in the security products as discussed in Chapter 6.

The objective of Phase 3 is to evaluate the security and efficiency of the new lightweight block cipher. This research implemented cryptanalysis tests that include avalanche effect, randomness test, and cryptanalysis attacks that are presented in Chapter 7. These cryptanalysis tests are useful and significant to measure the strength of lightweight block ciphers. Apart from that, software performance tests were conducted in Chapter 8 which includes execution speed and throughput evaluations to measure the efficiency of the new algorithm.

In conclusion, the three phases in the research methodology are aligned with the research objectives and be able to answer all of the research questions. The research processes in each phase are sufficient in achieving the research contributions and at the same time addressing the problem statement found in the early stage of the research.