K. J. Somaiya College of Engineering, Mumbai-77
(A constituent college of Somaiya Vidyavihar University)

Batch: B1	**Roll No.: 16010121045**
Experiment No 1	
Group No: 1	

Title: Prepare problem specification related to your mini project

Objective: Prepare problem definition of a Mini project

Expected Outcome of Experiment:

	At the end of successful completion of the course the student will be able to
CO1	Define the problem statement and scope of problem
CO2	Identify various hardware and software requirements for problem solution
CO5	Prepare a technical report based on the Mini project.

Books/ Journals/ Websites referred:

1.
2.
3.

Introduction:

As studied in Software Engineering, developing a successful product (software: including the code and documents) needs a systematic approach. In this experiment you will prepare the basic documents required to develop a product, a software system, a website or a mobile app to provide certain services or facilities.

Students will be required to prepare a document specifying.

Problem statement:

The challenge lies in creating a truly random number generator that guarantees high entropy and unpredictability. Traditional pseudorandom number generators (PRNGs) are deterministic and can be susceptible to predictability, which is undesirable in applications such as cryptography, security, and simulations that demand genuinely random sequences. The goal is to address the limitations of current PRNGs and develop a system that leverages both software-based advanced algorithms and hardware-based entropy sources to generate truly random numbers.

Motivation:

The motivation behind this project arises from the imperative need for true randomness in critical applications where security, reliability, and unpredictability are paramount. Traditional pseudorandom number generators (PRNGs) fall short due to their deterministic nature, rendering them susceptible to predictability and potential exploitation, particularly in cryptographic contexts. The project seeks to address this vulnerability by aiming to develop a random number generator that combines cutting-edge software algorithms with hardware-based entropy sources. The primary motivation is to mitigate security concerns, especially in cryptographic applications, where the predictability of random numbers poses a significant threat. Additionally, the project aims to enhance the entropy of generated numbers, making them suitable for simulations and modeling scenarios that require accuracy in representing real-world variability. By avoiding predictable patterns inherent in deterministic PRNGs, the project aspires to create a system that exceeds industry standards for randomness, ensuring robustness and reliability across diverse applications and domains.

Objectives of the project:

1. **Algorithm Implementation:**
    - Develop and integrate cutting-edge algorithms for random number generation within the software component. These algorithms should exhibit superior entropy and unpredictability, addressing the limitations of traditional pseudorandom number generators.
2. **Hardware Integration:**
    - Successfully incorporate hardware-based entropy sources into the system. By doing so, the project aims to enhance the randomness of generated numbers, adding an extra layer of unpredictability.
3. **Cryptography Integration:**
    - Enable the use of generated random numbers for cryptographic applications. The objective is to ensure a high level of security by providing truly random numbers, which is crucial for cryptographic protocols, key generation, and other security-sensitive operations.
4. **Statistical Evaluation:**
    - Implement robust statistical evaluation methods to assess the quality of the generated random numbers. The goal is to validate that the generated

sequences adhere to the criteria of true randomness, meeting or exceeding industry standards.

5. **Documentation and Reporting:**

    - Provide comprehensive documentation detailing the implemented algorithms, hardware components, and evaluation methodologies. Clear and concise reporting is essential for transparency, reproducibility, and future development.

6. **Security Assurance:**

    - Ensure that the system is resistant to potential attacks or exploitation, particularly in scenarios where the generated random numbers are used for cryptographic purposes. This involves considering both software and hardware security measures to safeguard the integrity of the random number generation process.

Scope of the project:

The project encompasses the following key components:

Software-Based:

Advanced Algorithms: Implement cutting-edge algorithms for random number generation that demonstrate superior entropy and unpredictability.

Cryptography: Focus on applications requiring robust random numbers for cryptographic purposes, where predictability could pose significant security risks.

Research-Based:

Hardware Integration: Explore and implement hardware-based entropy sources to enhance the randomness of generated numbers.

Hardware Security: Ensure that hardware components used in the system are secure and resistant to tampering or exploitation.

Randomness Evaluation:

Statistical Properties: Develop mechanisms to evaluate the statistical properties of the generated random numbers, ensuring they meet the required standards for true randomness.

Hardware requirements (for development)

1. **Development Machine:**
    - *Justification:* A high-performance development machine with a modern multi-core processor, sufficient RAM (16GB or more), and ample storage space is crucial for efficient software development, compilation, and testing.
2. **Random Number Generator Hardware Module:**
    - *Justification:* A dedicated hardware module capable of generating true randomness is essential for testing and integrating hardware-based entropy sources into the random number generation system.

Software requirements (for development) (Tech Stack)

1. **Programming Language: Python:**
    - *Justification:* These languages provide a balance between performance and rapid development (Python), making them suitable for both algorithm implementation and system integration.
2. **Version Control System: Git:**
    - *Justification:* Git enables collaborative development, version tracking, and code management, essential for a project with multiple contributors.
3. **Integrated Development Environment (IDE):**
    - *Justification:* An IDE like Visual Studio Code, PyCharm, or Eclipse provides tools for code editing, debugging, and project management, enhancing the development workflow.
4. **Simulation Tools:**
    - *Justification:* Simulation tools may be needed to emulate hardware-based entropy sources and evaluate the system's behavior under various conditions.
5. **Security Tools:**
    - *Justification:* Security testing tools and frameworks will be essential to identify and mitigate potential vulnerabilities in the code and system.

Hardware and software requirements (for deployment)

1. **Server Infrastructure:**
    - *Hardware Justification:* Depending on the scale of deployment, servers with sufficient processing power, memory, and storage should be selected. Cloud services like AWS, Azure, or Google Cloud may be utilized for scalability.
    - *Software Justification:* Deploy the random number generation system on a secure and well-configured server environment.
2. **Operating System: Linux (e.g., Ubuntu):**
    - *Hardware Justification:* Linux is a preferred choice for server environments due to its stability, security features, and open-source nature.
    - *Software Justification:* The chosen Linux distribution will serve as the operating system for the deployment environment.
3. **Web Application (Optional):**
    - *Hardware Justification:* If developing a web application, a web server (e.g., Apache or Nginx) may be required.
    - *Software Justification:* Use frameworks like Django (Python), Ruby on Rails (Ruby), or Express.js (JavaScript) for web application development.
4. **Database (Optional):**
    - *Hardware Justification:* For data storage, consider database servers (e.g., PostgreSQL, MySQL).
    - *Software Justification:* Utilize a database management system to store and retrieve data efficiently.

Type of Application: Web / PWA/ Desktop/ Mobile (Android)/other

Desktop based application.

References:

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9923932

https://www.nature.com/articles/s41598-021-95388-7

https://www.hindawi.com/journals/ddns/2019/2545123/

https://link.springer.com/chapter/10.1007/11569596_23

Plan:

Planning is very essential for successful completion of any activity in which multiple stakeholders are involved. To start with one will write down all activities needed to be carried out mentioning the role and responsibility of each human resource. This will also help in sequencing and tracking the progress of the development process. A sample Role and Responsibility matric could be as follows, Please prepare according to needs of your project.

Activity	R1	R2	R3	Mentor
1. Requirement Gathering				
1.1 Interaction with customer	R	R	R	A
1.2 Preparing SRS	C	C	C	A
2. Design				
2.1 Preparing Block diagram	C	C	R	A
2.2 Writing Functional Requirements	C	R	C	A
2.3 Writing Non-Functional Requirements	C	R	R	A
2.4 Developing Use Case	R	C	R	A
2.5 Developing Test Cases	R	C	C	A
3. **Planning**				
4. **Coding**				
4.1 Unit 1	C	R	E	A
4.2 Unit 2	C	R	E	A
4.3 Front end/ UI	E	R	E	A
5. **Testing**				
5.1 Unit 1	R	A	E	
5.2 Unit 2	R	A	E	
5.3 System Testing	A	R	E	A

C: Creator, R: Reviewer, A: Approver E: Executor

Conclusion:

In summary, the project aims to revolutionize random number generation by blending cutting-edge algorithms and hardware-based entropy sources, ensuring heightened security and unpredictability. The comprehensive approach encompasses algorithmic advancements, cryptographic integration, robust statistical evaluation, and stringent security measures.