QUANTUM BASED GENERATION OF CRYPTOGRAPHICALLY SECURE NUMBERS

PROBLEM STATEMENT

DEVELOP A QUANTUM RANDOM NUMBER GENERATOR SPECIFICALLY DESIGNED FOR CRYPTOGRAPHIC APPLICATIONS. EXPLORE METHODS TO ENHANCE THE SECURITY OF CRYPTOGRAPHIC SYSTEMS BY INCORPORATING QUANTUM-GENERATED RANDOM NUMBERS. PARTICIPANTS SHOULD FOCUS ON ENSURING THE UNPREDICTABILITY AND TAMPER-RESISTANCE OF THE GENERATED RANDOM VALUES.

INTRODUCTION TO QUANTUM COMPUTING

Quantum computing leverages principles of quantum mechanics to perform computations using quantum bits or qubits, which can exist in multiple states simultaneously. This allows quantum computers to potentially solve certain complex problems much faster than classical computers.

WHAT IS CRYPTOGRAPHICALLY SECURE NUMBERS ?

In simple terms, a cryptographically secure number is a random number that's created in a way that makes it really hard for someone to predict or manipulate. These numbers are important in security because they help keep things like passwords and confidential information safe from being easily guessed or hacked.

IMPORTANCE

- **Security in Cryptographic Applications**

Secure random number generation is essential for cryptographic protocols to prevent hacking and ensure data integrity.

- **Quantum Resistance**

QRNG provides resistance against attacks based on traditional random number generation algorithms.

- **Key Material Generation**

It plays a critical role in the creation of cryptographic keys with enhanced security.

WHAT IS QUBIT?

A qubit, short for quantum bit, is the fundamental unit of quantum information in quantum computing. Unlike classical bits, which can be either 0 or 1, qubits can exist in multiple states simultaneously, thanks to the principles of quantum superposition. This property allows quantum computers to perform complex computations more efficiently than classical computers for certain tasks.

IMPLEMENTATION

1. **Create Qubits:** Start with n quantum bits (qubits).
2. **Perform Operations:** Apply quantum operations or gates to manipulate the qubits and put them in a superposition of states..
3. **Measure Values:** Perform a measurement on the qubits, and the outcomes become your random number.

It's the inherent unpredictability of quantum states during measurement that provides the randomness in the generated numbers and the number of bits initialized which create more possibilities.

THANK YOU

SHASHANK A PATIL

KRISHNA AGGARWAL

JAVIN TRIVEDI