**Quantum-Secure Task Management & Communication in Space Networks**

With the advancements in quantum computing, traditional cryptographic methods face the risk of being compromised. This project aims to develop a **Quantum-Secure Task Management & Communication System** for satellite networks using **post-quantum cryptographic algorithms** integrated with an **LLM-driven key management framework**. The system will ensure secure inter-node communication and real-time task coordination while being resistant to quantum attacks.

The encryption process will involve **lattice-based key exchange (CRYSTALS-Kyber), post-quantum digital signatures (Dilithium), and hybrid AES-Kyber encryption** to safeguard task data and inter-satellite communications. Additionally, **LLM-powered blockchain-based key distribution** will be implemented to manage cryptographic keys securely across decentralized nodes. The LLM will also monitor satellite task logs to detect anomalies and initiate automated security adjustments.

**Software & Hardware Requirements**

**Software Requirements:**

* Python 3.x
* OpenAI GPT / Hugging Face Transformers
* PyCryptodome & NIST PQC Libraries (Kyber, Dilithium, Falcon)
* Linux/Windows environment

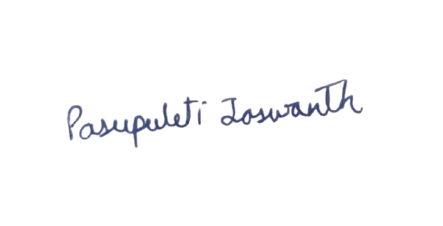
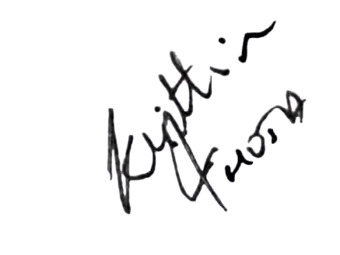
**Hardware Requirements:**

* Processor: Intel i5 or higher
* RAM: 8GB or higher
* Storage: Minimum 20GB free space
* Cloud or On-Prem GPU for LLM inference
* Quantum simulator (Optional for testing post-quantum resilience)

**References**

[1] Mengjiao Quan et al., "Constellation Encryption Design Based on Chaotic Sequence and the RSA Algorithm," Electronics, October 2022.  
[2] Farrukh Bin Rashid et al., "Privacy-Preserving for Images in Satellite Communications: A Comprehensive Review of Chaos-Based Encryption," arXiv, October 2024.  
[3] Anju Rani et al., "Combined Quantum and Post-Quantum Security for Earth-Satellite Channels," arXiv, February 2025.  
[4] Chaoyu Zhang et al., "StarCast: A Secure and Spectrum-Efficient Group Communication Scheme for LEO Satellite Networks," arXiv, February 2025.  
[5] Hanshuo Qiu et al., "Securing Satellite Communications: Real-Time Video Encryption Scheme on Satellite Payloads," arXiv, March 2025.  
[6] Mohamed Elmahallawy et al., "Secure and Efficient Federated Learning in LEO Constellations using Decentralized Key Generation and On-Orbit Model Aggregation," arXiv, September 2023.  
[7] Yijun Deng et al., "Security Transmission Technology for Satellite Communication Based on Integer Domain Chaotic System," Proceedings of SPIE, May 2022.  
[8] K. Das and P. Debnath, "Exploring Post-Quantum Cryptography: Review and Directions for Future Research," Technologies, December 2024.  
[9] X. Zhang et al., "PQNTRU: Acceleration of NTRU-based Schemes via Customized SIMD Processor," IACR Cryptology ePrint Archive, 2024.  
[10] S. Patel and R. K. Gupta, "A Meta-Analysis on NIST Post-Quantum Cryptographic Primitive Finalists," Journal of Emerging Investigators, 2023.

**Reg. No | Name of the Student | Signature**

BL.EN.U4AIE22046 | Pasupuleti Jaswanth|   
BL.EN.U4AIE22064 | Vangapandu Baladitya|   
BL.EN.U4AIE22026 | Krithin Thota] |

BL.EN.U4AIE22010| Dhanush Dayanand | 