**Internship Progress Report**

**Intern Details**

* **Name: Swarn Ranjan**
* **Internship Duration: 06th May 2025 – 30th June 2025**
* **Institution: Kalinga Institute of Industrial Technology**
* **Mentor: Dr. Tarun Yadav, Scientist-F, SAG, DRDO, New Delhi**
* **Reporting Period: Week 2 (06/05/2025 – 20/05/2025)**

**1. Topics Covered**

**During the period under review of the internship, the focus was on building foundational knowledge of cryptology and its applications. The topics explored include:**

* **Differences between cryptology, cryptography, and cryptanalysis**
* **Structure and function of HTTPS, and the role of TLS/SSL protocols**
* **Stages of the TLS handshake**
* **Principles of symmetric and asymmetric cryptography**
* **Concepts of public and private keys**
* **Use and characteristics of hash functions**
* **Purpose and implementation of digital signatures**
* **Basics of blockchain technology and cryptocurrency systems**
* **Introduction to major cryptographic algorithms: DES, AES, RSA, and Diffie–Hellman**

**2. Resources Utilized**

**A combination of official documentation, educational platforms and textbooks were used to study the above concepts. Key resources include:**

1. **IBM Docs – Overview of cryptographic principles, symmetric/asymmetric keys, and hashing**
2. **OWASP – Explanation and examples of cryptanalysis techniques**
3. **Cloudflare Learning – Description of HTTPS and TLS security features**
4. **Wikipedia – In-depth coverage of the TLS handshake, DES, AES, RSA, and Diffie–Hellman**
5. **Cryptography.io – Insights into symmetric encryption and cryptographic hash functions**
6. **CISA (Cybersecurity & Infrastructure Security Agency) – Digital signature fundamentals**
7. **Alchemy University – Blockchain basics, consensus models, and crypto mechanisms**
8. **William Stallings, *Cryptography and Network Security* – Chapters 1–4**
9. **Stephen Thomas, *SSL/TLS Essentials* – Overview of secure web communication protocols**

**3. Key Learnings**

* **Cryptology vs. Cryptography vs. Cryptanalysis  
  Cryptology is the overarching study of secure communication. It includes cryptography (techniques for secure communication) and cryptanalysis (methods for analyzing and breaking those techniques).**
* **HTTPS and TLS/SSL  
  HTTPS integrates HTTP with TLS/SSL encryption, providing confidentiality and integrity in data transfer. TLS replaces older SSL protocols in most modern implementations.**
* **TLS Handshake  
  The TLS handshake is a multi-step process where the client and server exchange information, agree on cryptographic parameters, and establish session keys before securely transmitting data.**
* **Symmetric vs. Asymmetric Cryptography  
  Symmetric encryption (e.g., DES, AES) uses a shared key for both encryption and decryption. Asymmetric encryption (e.g., RSA, Diffie–Hellman) uses a public/private key pair, enabling secure key exchange and digital signatures.**
* **Public and Private Keys  
  Asymmetric systems involve a public key (used to encrypt) and a private key (used to decrypt or sign), allowing for secure communication and identity verification.**
* **Hash Functions  
  Hash functions produce a fixed-length digest from input data. They are essential for ensuring data integrity and are commonly used in password storage, digital signatures, and blockchain.**
* **Digital Signatures  
  Digital signatures use a combination of hashing and private key encryption to verify the authenticity and integrity of a message or document.**
* **Blockchain and Cryptocurrency  
  Blockchains serve as decentralized, tamper-resistant ledgers secured by cryptographic hashing. Cryptocurrencies, such as Bitcoin, rely on blockchain technology to enable peer-to-peer value transfer.**
* **Data Encryption Standard (DES)  
  DES is a symmetric-key algorithm that uses a 56-bit key and operates through 16 rounds of processing. It is now considered outdated due to vulnerability to brute-force attacks.**
* **Advanced Encryption Standard (AES)  
  AES is a symmetric cipher widely adopted for its efficiency and strong security. It supports key sizes of 128, 192, and 256 bits, and is used in applications ranging from secure messaging to government data protection.**
* **Rivest–Shamir–Adleman (RSA)  
  RSA is an asymmetric encryption method commonly used for securing sensitive data, digital signatures, and certificate verification. It is based on the difficulty of factoring large primes.**
* **Diffie–Hellman Key Exchange  
  Diffie–Hellman enables two parties to establish a shared secret over an insecure channel without prior knowledge. It forms the basis of many secure communication protocols.**

**4. Upcoming Objectives (Weeks 3–4)**

* **Implementation of AES or DES in Python/C**
  + **Study official specifications: FIPS 197 (AES), FIPS 46-3 (DES)**
  + **Design and code encryption and decryption routines**
  + **Use test vectors to validate outputs**
* **Testing and Documentation**
  + **Build unit tests for each module (key schedule, round functions, etc.)**
  + **Add a README file with working examples and usage instructions**
  + **Optionally, include support for ECB and CBC encryption modes**
* **Further Exploration**
  + **Explore SHA-based integrity verification (if time permits)**
  + **Begin planning the secure chat application project phase**

**(Swarn Ranjan)**