# PRATHAMESH DHAKE

**Graduate Student, Boston University**

@ PrathamD_Sec@proton.me  Prathamesh Dhake  I-9028  617-560-0113

## EDUCATION

| Qualification | Specialization | Institute | Year | CPI/% |
|---|---|---|---|---|
| MS | *Computer Science* | Boston University | 2024-Present | 3.89/4.00 |
| B.Tech | *Electrical Engineering* | Indian Institute of Technology, Bombay | 2019-2023 | 7.13/10 |

## SKILLS

**Programming Languages:** Python | C++ | Bash Scripting | R | Rust | MATLAB

**Frameworks & Technologies:** LaTeX | Git | SageMath | Systemd | Docker

**Security Tools:** Wireshark | Autopsy | Metasploit | nmap | Qualys | Splunk

**Operating Systems:** Linux | Windows

## CERTIFICATIONS

**Certified in Cybersecurity (CC)** — *ISC2 [Feb, 2025]*

**Red Hat Certified System Administrator (RHCSA)** — *Red Hat, Expected: [May, 2025]*

**Qualys Vulnerability Management Specialist** — *Qualys, Expected: [April, 2025]*

## PROFESSIONAL EXPERIENCE

### Coupa Software India Pvt. Ltd.

*Software Engineer Intern*

- Gained a solid understanding of gem sets and the management of Ruby on Rails applications.
- Upgraded an application across multiple Ruby versions while ensuring gemset compatibility.
- Migrated a Docker-based Invoice Compliance Service to a cloud-based CCP Kubernetes

## B.TECH. PROJECT

### Cryptoanalysis of ciphers by black box approach to local inversion

- The project aimed to analyze the computational efforts to recover the key using a new black box approach in cryptography. We analyzed stream ciphers such as RC4 and block ciphers such as AES.
- Calculated the Linear Complexity of various bit sequences multiple times to compute the minimal polynomial for key retrieval.

## LEADERSHIPS & ACTIVITIES

### Clipboard Management on Linux

- Engineered a secure Wayland-based Clipboard History application for Linux with POSIX-compliant shell scripts and PEP8-standard Python code, implementing proper system hardening techniques
- **Architected** a custom systemd service with principle of least privilege, minimizing attack surface by restricting clipboard data to plain text only

### Speeding up scalar multiplication over Elliptic Curves

- Designed and implemented a custom secure data type for handling cryptographic parameters on NIST P-Curves
- Optimized ECC operations by developing parallel processing algorithms using numba and numpy, with comprehensive performance analysis via Scalene

### Security for the Internet of Things

- Analyzed multi-layer security protocols and communication vulnerabilities in IoT ecosystems, focusing on encryption implementation challenges
- Evaluated resource constraints for implementing Elliptic Curve Cryptography in IoT environments, proposing optimization techniques for secure communications

### Self-synchronizing Stream Cipher Analysis

- Developed custom state update functions and constructed reduced analogs of Self-Synchronizing ciphers to test cryptographic strength
- Utilized SageMath to conduct linear complexity profiling across multiple initialization vectors, identifying potential weaknesses in stream cipher implementations

### Practical Implementation of ElGamal and RSA Cryptosystems

- Engineered secure implementations of ElGamal and RSA algorithms with proper key generation, encryption, and decryption capabilities
- Executed comprehensive unit testing with near-complete code coverage, including simulation of various attack scenarios to verify cryptographic integrity

### Comparative Study of OS Kernel Random Number Generators

- Conducted security analysis of cryptographically secure random number generation implementations across Windows, Linux, and MacOS kernels
- Evaluated entropy sources and seeding mechanisms critical to system-wide security, documenting improvements in modern kernel RNG designs

### Investigation of Spectre-Class Side-Channel Attacks and Linux Kernel Mitigations

- Analyzed side-channel attack vectors alongside Linux kernel mitigation techniques, including kernel page-table isolation and retpoline implementations
- Demonstrated a practical proof-of-concept for Spectre v2 vulnerability exploitation in Linux environments, documenting security implications

## EXTRA-CURRICULAR ACTIVITIES

- Built an Android app interfaced, HC-05 module-based Bluetooth-controlled robot. *(2019)*
- Part of an 8-member team that organized the International Micromouse Challenge at TechFest IIT Bombay. *(2019)*
- Successfully completed a course on Teaching Assistants Skill Enhancement & Training. *(2023)*