# HIRAK MONDAL

2nd Year Postgraduate
Department of Computer Science and Engineering, IIT Kanpur
hirakm20@iitk.ac.in
+91 7003347082

## Academic Qualifications

| Year | Degree/Certificate | Institute | CPI/% |
|---|---|---|---|
| 2020 - Present | M.Tech. (CSE) | Indian Institute of Technology, Kanpur | 8.00/10 |
| 2020 | B.Tech. (CSE) | University of Engineering and Management, Kolkata | 9.17/10 |
| 2016 | HSE West Bengal State Board | Patha-Bhavan, Kolkata | 83.40% |
| 2014 | SE West Bengal State Board | Patha-Bhavan, Kolkata | 88.40% |

## Master Thesis Project

- **$P^3$-AID: PUF based Privacy Preserving Authentication for Internet of Drones** | Guide: Dr. Urbi Chatterjee (*March'21-Ongoing*)
  - Working on lightweight unique identification mechanism of the UAV platforms
  - Devising efficient key management of thousands of such platforms in case deployed in large scale
  - Implementing an FPGA based PUF design and developing a privacy-preserving anonymous authentication protocol with the companion embedded computer

## Course Projects

- **Encryption and Decryption Scheme for Software Security** | Modern Cryptology (CS641) (*Jan'21-May'21*)
  Performed cryptanalysis and implemented several software-based encryption techniques, some are listed below:
  - Implemented Substitution Cipher
  - Implemented Playfair Cipher
  - Implemented 6-Round DES
  - Implemented RSA Encryption
- **Network Vulnerabilities and Web Exploitation** | Computer Systems Security (CS628A) (*Jan'21-May'21*)
  Performed various Network and Web attacks, in the *rootsh3ll* Lab, given below is the list of the same :
  - Performed reconnaissance with Nmap to reveal hidden secrets
  - Gathered Information of live wireless and wired network data
  - Performed Live Network Traffic Analysis
  - Monitored wireless traffic and filtered out useful information using Monitor Mode
  - Analyzed Wireless LAN Protocols
  - Explored sample packet capture files to extract useful information about network, clients, and traffic
  - Exploited MySQL vulnerability by exfiltrating employee data from organization's database
  - Performed packet analysis on live network traffic using SQL Injection
  - Performed Cross-Site Request Forgery attack
  - Performed XSS attacks
- **Multi-level Cache Simulation** | Advanced Computer Architecture (CS622A) (*Sep'20-Oct'20*)
  - Simulated L1 cache misses through L2, L3 cache hierarchy for various applications
  - Implemented 3 types of Cache Policies- Inclusive, Exclusive, and NINE
  - Simulated 8-way LRU Level 2 cache and 16-way LRU level 3 cache
  - Simulated 8-way LRU Level 2 cache and Fully Associative LRU level 3 cache
- **Non-Cache Model Architectures and CDF Analysis** | Advanced Computer Architecture (CS622A) (*Oct'20-Nov'20*)
  - Conducted studies to understand the reuse and sharing profiles of a set of parallel program
  - Instrumented these shared-memory parallel programs using PIN and captured the per-thread memory access traces
  - Analyzed the traces of four programs by simulating a machine with no cache
  - Analyzed our results on that cache less simulated system and derived the Cumulative Density Function of the misses
  - Gained insights from the analysis and introduced a cache in our simulation model, trying to observe how by this new change the system is benefited

## Technical Skills

- **Languages:** C, C++, Familiarity with- Python, MySQL, Java
- **Tools & Frameworks:** OpenMP, CUDA, IntelTBB, Intel MPI, Intel Pintool, Nmap, Wireshark, LaTeX

## Position of Responsibility & Scholastic Achievements

- Teaching Assistant, Fundamentals Of Computing (ESC101), IIT Kanpur (*Jul'21-Present*)
- Secured AIR 111 in JEST 2020 Theoretical Computer Science Examination (*Feb'20*)

## Relevant Courses

Advanced Computer Architecture (CS622A)
Modern Cryptology (CS641A)
Computer Systems Security (CS628A)
Programming for Performance (CS610A)
Introduction to Machine Learning (CS771A)
Parallel Computing (CS633A)