Amir Matin Shahnazi

B.Sc. in Computer Science, Sharif University of Technology (Expected Feb 2026)

Email: shahnaziamirmatin@gmail.com | GitHub: matinshaah

Education

Sharif University of Technology, Tehran, Iran   Expected Feb 2026
Bachelor of Science in Computer Science
GPA: 18.68 / 20
Ranking: 7 / 44 (Top 15%)
Full Grade Report: View Here

Relevant Coursework

Introduction to Cryptography	**Topics in Cryptology**
Lattice-Based Cryptography	**Advanced Topics in Alogirthms**
Data and Network Security	Computer Networks
Theory of Computation (audited)	Automata Language Theory
Probability and Statistics	Artificial Intelligence
Analysis of Algorithms	Data Structures
Numerical Analysis	Math Logic
Operating Systems	Principles of Computer Systems
Computer Technology	Database Design

Teaching Assistantships

- **Introduction to Cryptography** — Teaching Assistant

- **Data Structures** — Teaching Assistant; **Head TA**

- **Analysis of Algorithms** — Teaching Assistant

- **Computer Networks** — Teaching Assistant

- **Discrete Mathematics** — Teaching Assistant

- **Advanced Programming** — Teaching Assistant

Research & Academic Experience

Paper Review: *Post-Quantum Homomorphic Encryption: A Case for Code-Based Alternatives*
- Conducted literature review and analysis of post-quantum fully homomorphic encryption schemes.
- Compared code-based cryptographic constructions for security and performance.

Workshops & Training

- *School of Post-Quantum Cryptography*, Isfahan University — Ordibehesht 1404 (May 2025). Covered lattice-based and code-based cryptography (encryption, key exchange, and digital

signatures), hash-based signature schemes, and an overview of NIST PQC finalists and standards.

- *IPM Workshop on Post-Quantum Cryptography* — 2025.
  Topics included quantum computing fundamentals, hash-based cryptography, isogeny-based schemes, Euclidean lattices and their applications, code-based cryptography, and an introduction to multivariate-based schemes.

Work Experience

Software Engineer (Backend) — Tabdeal Crypto-Exchange, Tehran, Iran [Feb 2024 – Dec 2024]
- Developed and maintained backend systems for cryptocurrency exchange operations.
- Worked with blockchain-related data structures, APIs, and secure transaction processing.
- **Technologies:** Java, Go, Python, Django, Java Swing

Technical Skills

Programming:	Java, Go, Python, R, Matlab
Frameworks/Tools:	Django, JavaSwing
Concepts:	Cryptography, Algorithms, Backend Development, Software Engineering

Languages

Persian (Native), English (TOEFL iBT 98)

Research Interests

Post-Quantum Cryptography; Lattice-Based Cryptographic Schemes; Fully Homomorphic Encryption; Data and Network Security