David Hacker

dmhacker@protonmail.com • dmhacker.github.io

Education

- **University of California San Diego** — **La Jolla**
  Major: Computer Science, Minor: Mathematics, 3.94 — *2017–2021*

Work Experience

Positions Held

- **University of California San Diego** — **La Jolla**
  CSE Department Tutor — *April 2018–July 2018, September 2018–Present*
  - Helped teach CSE 20, Discrete Mathematics under Professor Daniele Micciancio
  - Currently teaching CSE 21, Mathematics & Systems Analysis under Professor Quang Bach
  - Held office hours on a weekly basis and provided tutoring to students who required additional help
  - Graded students' homework assignments, midterms and final exams

- **Medspace** — **La Jolla**
  Software Engineering Intern — *February 2018–September 2018*
  - Wrote a command line tool in C# to import 166 million rows of CSV data into a Neo4j graph database
  - Created an ASP.NET Core backend & RESTful API to interface with the database
  - Implemented an k-dimensional tree in the backend to speed up geospatial queries by a factor of several hundred
  - Managed nearly $20,000 worth of server resources, used to store data and host the backend
  - Designed another backend using the Java Spring framework to supply customers with medical analytics
  - Integrated an Auth0 authentication system into the Spring backend to protect user data

Notable Projects

- **RLWE Cryptography:** *C++, Number Theoretic Library*
  - Implemented several prominent post-quantum cryptosystems related to the ring learning with errors (RLWE) problem
  - Designed a fast version of the Fan-Vercauterean cryptosystem, allowing for computations on encrypted data
  - Additionally integrated Peikert-style key exchange & Ring-TESLA digital signature algorithms
- **Dual_EC_DRBG Backdoor:** *Rust, GNU Multiple Precision Arithmetic*
  - Demonstrated how a Shumlow-Ferguson attack could be used to break a dual elliptic curve random number generator
  - Heavily optimized the attack by writing custom implementations for NIST P-256, P-385, and P-521 elliptic curves
  - Can determine a generator's internal state in roughly 20 seconds using an i7-8650U processor
- **Decentralized Email:** *NodeJS, Forge Cryptographic Library, Truffle*
  - Used the Ethereum blockchain as a means to store encrypted messages of variable length
  - Integrated AES & RSA cryptosystems to ensure that messages could be transmitted between users safely
  - Worked on a team with three others to design the application over the course of several months
- **Alexa YouTube Skill:** *NodeJS, FFmpeg, AWS Lambda, Heroku*
  - Created a skill that lets Amazon Alexa devices play audio from YouTube videos as a hobbyist project
  - Downloaded over 3000 times and has over 100 stars on GitHub
  - Reviewed by the German tech channel Venix, which has over 10,000 subscribers

Technical Skills

- **Languages:** C, C++, C#, Rust, Java, Python, JavaScript, Solidity, ARM Assembly
- **Frameworks:** MEAN stack, Flask, Spring, ASP.NET Core, Materialize, React Native
- **Databases:** MongoDB, Neo4j, Redis, Firebase, MySQL