

Nolan CAROUGE

✉ nolan.carouge.pro@gmail.com ☎ 07 67 48 64 09 🔗 nolancarouge.fr 🐙 [carougen](https://github.com/carougen)
🌐 [nolan-carouge](https://nolan-carouge.com)

Education

Grenoble INP - Ensimag, Engineering degree (CS & Applied Math) – Grenoble, France Sept 2023 – June 2026

- Information Theory, Probability, Statistics, Numerical Analysis, Algorithms, Networks, Security, Programming, and Processor Design. Year 2 at KU Leuven. Year 3 aligned with UGA CySec double degree.

Université Grenoble Alpes, CySec (M2) - Double degree – Grenoble, France Sept 2025 – June 2026

- Advanced Cryptography, Secure Architectures, Software & Physical Security, Audit & Risk.

KU Leuven, Erasmus - Master courses in Cybersecurity – Leuven, Belgium Sept 2024 – June 2025

- Semester 1 : Cryptography, Secure Software, AI, Secure Systems. Semester 2 : Advanced Cryptography, Computer Algebra, Deep Learning & Hardware Security.

Grenoble INP - ESISAR, Preparatory cycle – Valence, France Sept 2021 – June 2023

- Foundations in CS (Algorithms, Networks, Python/C/Haskell), Mathematics, Physics, and Engineering.

Experience

Intern, eShard – Bordeaux area, France - On-site - eshard.com July 2025 – Aug 2025

- EM side-channel research on ReLU-based neural nets on STM32.
- Built firmware and automated leakage mapping, identified leakage points and created classifier using statistical methods.

Intern, KU Leuven (Prof. Mathy Vanhoef) – Leuven, Belgium - Hybrid Oct 2024 – Mar 2025

- Extended **OpenSnitch** to flag/mitigate risky LAN connections Ref: [OpenSnitch proposal](#).
- Improved **LANShield** (Android) with finer filtering and notifications.
- Built a Python POC for a new type of protocol to access a LAN.

Web Developer, Entente Natation Pierrelatte (Freelance) – Remote - May 2024 – Sept 2024
natation-pierrelatte.fr

- Rebuilt the club website with online registration, payments, health forms, discounts, and booking.
- Designed an admin panel and QR-code attendance system, built with **Django**.

Selected Projects

Homomorphic RLWE 2025

- Exploration of Ring-Learning-With-Errors for homomorphic encryption, secure computation over encrypted data.

Bitcoin-like Blockchain 2025

- Simplified blockchain with transaction validation and block mining.

Zero-Knowledge Proofs from Disequations 2025

- Implementation of ZK protocols based on disequations for privacy-preserving authentication.

AES Implementations (Haskell & C) 2024

- Complete AES implementation.

Graphics Interface Library in C 2024

- Graphics library from scratch, used to build 2048 and Minesweeper.

Awards

Excellence Scholarship - CyberAlps June 2025

- Awarded for academic performance (Grenoble INP - Ensimag).

Excellence Scholarship - Fondation INP

Jan 2025

- Awarded for academic performance (Grenoble INP - Ensimag).

Skills

Languages: C, Python, PHP, Haskell, Rust, Bash, Magma, HTML/CSS/JS, TypeScript, VHDL

Frameworks & Tools: Git/GitHub, Linux, LaTeX, Django, MATLAB, Sage

Security & Crypto: Cryptography, hardware & software security, CTF, Hack The Box, Root-Me