Jules **ROUSSEAU**

Profile

Former intern in the Irisa/Inria labs, I'm interested in software cryptography and development. After 6 months as research intern in lightweight symmetric cryptanalysis, I'm seeking a first experience in a company. Proficient in Python and C/C++, I appreciate implementation and I'm willing to improve my skills in this domain and apply them to concrete projects.

Contact details

@ jr.julesrousseau@gmail.com
☎ +336 51 03 43 73
🌐 julesrousseau.github.io
✉ 68 bd de Metz 35700 Rennes

Personal information

Year of birth: **2001**

Languages: **French** (native), **English** (B2/C1), **Spanish** (B1)

Driver license : **Permis B**

Skills

- Python & Sagemath, C & C++, Java, Solidity, LaTeX, Bash, Git
- MILP, SAT, Gurobi
- Symmetric cryptanalysis, Scientific research, Lightweight encryption
- Curious, Detail-oriented, Self-sufficient

Master's graduate in Cryptography seeking a position in Software/Security Engineering

Experience

Research intern at *Inria* in *CAPSULE team* **2024.04–2024.09**
▷ Lightweight symmetric cryptanalysis, Cube attacks, Integral distinguishers, MILP/SAT modelling of ASCON-128 and GIFT-64 ciphers
▷ Supervisors : André Schrottenloher, Patrick Derbez

Education

Master I & II Cryptography. Mathematical information theory, cryptography. *University of Rennes, Cyberschool.* **2022–2024**
▷ Security of Implementations (side channel analysis and code review), Symmetric and Asymmetric cryptanalysis, Network security, Lattices, Machine learning, Error-correcting codes, Elliptic curves, Quantum cryptography
▷ Options : C++ (basics + complements), Blockchain
▷ Mention Bien

Bachelor Mathematics. *University of Angers.* **2019–2022**
▷ Linear and bilinear algebra, Probabilities, Euclidean geometry, Rings and groups, Differential calculus
▷ Mention Assez Bien

Scientific Baccalaureate. Specialization in mathematics, *Lycée François Truffaut.* **2019**
▷ Mention Très Bien

Academic projects

DSA - Digital signature algorithm (Java) **Master II, 2023-2024**
▷ DSA implementation based on FIPS 186-3 standard
▷ Multi-precision library

Secured Messenger (Java) **Master II, 2023-2024**
▷ Sockets, Double-Ratchet Algorithm, Diffie-Hellman

AES implementation (C) **Master I, 2022-2023**
▷ Advanced Encryption Standard implementation based on FIPS 197 standard

Steganography (C) **Master I, 2022-2023**
▷ End of Master I project defended in May 2023, implementation of software program to hide images/text messages in PNG using different methods

Sudoku (C) **Master I, 2022-2023**
▷ Solving 64x64 Sudoku grid
▷ Heuristics and backtracking
▷ Valgrind

Hobbies

Sports: Climbing & Swimming
Cessna 172 Piloting: Aeronautical Initiation Certificate, Objective : obtain the Private Pilot License