Jules **ROUSSEAU**

PROFILE

Intern in the Irisa/Inria labs, in the Capsule team, I'm interested in Software cryptography. 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 as well as theory and I'm willing to improve my skills in both domains.

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), **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 student in Cryptography seeking a security engineering position

EXPERIENCE

RESEARCH INTERN at *Inria* in *CAPSULE team*   **2024.04–pres.**
▷ 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 FPGA 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