Reynaldo Caceres Villena

Email: reynaldocv@gmail.com
LinkedIn: linkedin.com/in/reynaldocv
GitHub: github.com/reynaldocv
Leetcode: leetcode.com/reynaldocv
Cellphone: +51 (11) 95000 9748

Education

University of São Paulo - Institute of Mathematics and Statistics — São Paulo, Brazil
Ph.D. in Computer Science, **GPA**: 8.7/10, **Adviser**: Routo Terada — Mar 2018–Oct 2024

- Thesis: "Attacks and Vulnerabilities on NewHope KEM and small-Ring-LWE problem"

National University San Antonio Abad of Cusco — Cusco, Peru
Ing. in Software Engineering and Informatics, **GPA**: 19/20, **Adviser**: Lauro Enciso — 2015

- Thesis: "Factoring any Integer with Random Bits"

University of São Paulo - Institute of Mathematics and Statistics — São Paulo, Brazil
M.S. in Computer Science, **GPA**: 8.5/10, **Adviser**: Routo Terada — Mar 2010–Set 2013

- Thesis: "Reconstructing the Secret Key of Multi-Prime RSA Cryptosystem"

National University San Antonio Abad of Cusco — Cusco, Peru
B.S. in Software Engineering and Informatics, **GPA**: 14/20 — Jul 2004 –Mar 2009

Skills

- **Cryptography & Data security**
- **Web development:** Php, Html, Javascript, Python & Django
- **Android development:** Android Studio & Java
- **Programming Languages:** Python, C++, C#, PHP, Java & Javascript
- **Databases:** SQL server, SQLite, MySQL server & Oracle server, .
- Experience with Windows and Linux.
- Regular Contestant at leetcode.com/reynaldocv

Languages

- **Spanish** (Native)
- **English** (Intermediate)
- **Portuguese**(Intermediate)

Courses taken

- **Ph.D.'s Program:** Internet of Things, Machine Learning, Digital Entrepreneurship, Development of computer systems, Principles of Human-Computer Interaction, Introduction to Graph Theory, Blockchain and Smart Contracts, Academic Writing.
- **Master's Program:** Algorithm Analysis, Data Structures, Languages, Automata and Computability, Artificial Intelligence, Concepts of Programming Languages, Introduction to Cryptology.

  Extra Credits: Computational Complexity, Knowledge-Based Systems.
- **W3schools:** Django, Data Science, Git.
- **Cousera:** An Introduction to Cryptography, Criptography I, Number Theory.

Experience

Museum of Contemporary Art, University of São Paulo — São Paulo, Brazil
Software Developer/Specialist in big and digital data — Set 2024–

- Collectiveaccess and Dspace repositories software programmer (PHP, MySql server & Gemini).

University of São Paulo — São Paulo, Brazil
(Researcher) Phd's program student/Institute of Mathematics and Statistics — Mar 2018–Oct 2024

- Study of some post-quantum cryptographic schemes (C++ & Python3).

Seguro Social de Salud - EsSalud/Ministry of labor — Cusco, Peru
Software Developer/Hospital I Urubamba — Jun 2015–Feb 2018

- Development of File Management & Auditing software (C#, PHP & MySql server).

Provincial Munincipality of Mollepata — Cusco, Peru
Software Engineer/Informatic Area — Jan 2014–Apr 2015

- Software developed for Warehouse Management. (C# & Sql server).

University of São Paulo — São Paulo, Brazil
(Researcher) Master's program student/Institute of Mathematics and Statistics — Feb 2010–Set 2013

- Software for recovering secret keys on variants of cryptosystem RSA (C++ & Python3).

Information Technology Services, Perú — Cusco, Peru
Software Engineer/Webpage Programming Area — May 2009–Feb 2010

- Web programming (CMS Joomla, PHP, HTML, CSS & MySql server).

Publications

[1] R. C. Villena and R. Terada, "Recovery of the secret on binary ring-lwe problem using random known bits-extended version", *Journal of Internet Services and Applications*, vol. 15, no. 1, pp. 39–45, 2024.

[2] R. Villena and R. Terada, "Recovering the secret on binary ring-lwe problem with random known bits", in *Anais do XXIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, Juiz de Fora/MG: SBC, 2023, pp. 534–539.

[3] R. Terada and R. C. Villena, "Vulnerability—information leakage of reused secret key in newhope", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 105, no. 6, pp. 952–964, 2022.

[4] R. Villena and R. Terada, "The importance of the public global parameter on ring-lwe problem-based key encapsulation mechanims", in *Anais do XXII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, Santa Maria: SBC, 2022, pp. 378–383.

[5] R. Terada and R. C. Villena, "Factoring a multiprime modulus n with random bits", in *Information Security: 16th International Conference, ISC 2013, Dallas, Texas, November 13-15, 2013, Proceedings*, Springer, 2015, pp. 185–196.

Teaching

- **Teaching Assistant** at Intitute of Mathematics and Statistics - University of Sao Paulo — Feb 2022 –Jun 2022
  Introduction to Cryptology

Some projects

See full list of projects on github.com/reynaldocv.

- Cronicos monitoring (link)
  Software to monitor chronic people. This web page helps to improve the monitoring of sick people, and manage their attentions, electrocardiograms in hypertensive people, foot cheek in diabetic people, references to a major hospital, and Mosare (Django, Python3, Javascript, CSS & SQLite).
- Web-Content-Analysis (link)
  Software to analyze inappropriate content of a web page. It uses Microsoft Microsoft Azure and Google Cloud services to analyze images and search words and phrases (Javascript).
- MAC6929-IoT-parking (link)
  Prototype software for parking management. This system returns the number of total free parking spaces. Use Machine Learning to know how many free sites there will be in the future (Python, Android Studio & Java).
- Leetcode (link)
  This repository contains solutions to problems on leetcode.com (Python3).

Scholarships and Awards

- Scholarship, for doctoral's studies, IME - USP 2018–2023
- Scholarship, for master's studies, IME - USP 2010–2012