[FALL 2025 585]

Project proposal: Salsa20

Nick Whiteman and Nathan Metens

Department of Computer Science
Portland State University

{*nicholaw, metens*}*@pdx.edu*

November 1, 2025

1 The topic: Implementing and Understanding the Salsa20 Stream Cipher

Cryptography is essential for securing modern communications, yet implementing it correctly remains challenging. In this project, we focus on the Salsa20 stream cipher, a fast and secure symmetric encryption algorithm designed by Daniel J. Bernstein. Salsa20 has influenced modern systems such as ChaCha20, used in TLS, VPNs, and secure messaging protocols. Our goal is to explore both the theoretical foundations and practical implementation of Salsa20—understanding its key generation, keystream process, and resistance to cryptographic attacks. By combining hands-on coding with research, we aim to highlight what makes Salsa20 an elegant and effective cipher for real-world use.

2 The goal

In this project, we aim to gain a deep understanding of the Salsa20 stream cipher by studying its design, implementation, and security properties. Specifically, we plan to implement Salsa20 in Python, test it with various input samples, and develop both the encryption and decryption functions to verify correctness. We will then analyze the cipher's strengths and potential vulnerabilities, exploring how misuse or poor parameter handling could compromise security. Our final deliverable will include a written analysis summarizing our findings, what we learned from the implementation process, and potential ideas for improving or extending Salsa20. We will also do a brief description of Salsa20's successor, ChaCha20, and why it replaced Salsa20. Core references for this work include Daniel J. Bernstein's original Salsa20 Family of Stream Ciphers paper [[9]], the Crypto++ Wiki [[10]], and the Libsodium documentation [[11]]

3 The plan

Work Plan and Timeline

To ensure steady progress. We plan to follow this schedule and division of responsibilities (although we will be doing many of these parts together).

- **Weeks 5–6:** Review the stream ciphers and Salsa20 encryption algortithm, finalize references, and submit the proposal by November 3.
- **Week 7:** Begin implementing Salsa20 encryption in Python and test functionality with sample plaintexts, keys, and nonces.
- **Week 8:** Implement and verify the decryption function, perform initial security tests, and be ready for the progress check.
- **Weeks 9–10:** Analyze performance, explore vulnerabilities, and prepare slides and code demonstrations for the in-class presentation.
- **Weeks 11–12:** Finalize results, complete the written report in LaTeX, polish the bibliography, and submit the final report by December 10.

Division of Responsibilities: Both of us will focus on the theoretical background and Python implementation of Salsa20. We will collaborate via GitHub and communicate weekly via Discord to coordinate tasks and ensure all milestones are met on time.

References

[1] Wikipedia contributors. "Salsa20." *Wikipedia, The Free Encyclopedia*. Available at: https://en.wikipedia.org/wiki/Salsa20. Accessed October 25, 2025.

[2] Johnlwhiteman. "Cryptography Repository." *GitHub*. Available at: https://github.com/johnlwhiteman/cryptography. Accessed October 25, 2025.

[3] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Third Edition. CRC Press, 2021.

[4] Daniel J. Bernstein. Available at: https://cr.yp.to/snuffle/salsafamily-20071225.pdf. Accessed October 31, 2025.

[5] OpenAI, *ChatGPT (GPT-5)*, Oct. 22, 2025. [Online]. Available at: https://chat.openai.com/

[6] Computerphile. "Salsa20 – Cipher." YouTube, 11 July 2019, https://www.youtube.com/watch?v=1pheUuX8f0U. Accessed 31 Oct. 2025.

[7] Christof Paar. "Stream cipher: Two-time pad, RC4, CSS, Salsa20." YouTube, 17 May 2020, video, 1 h 23 m 45 s, posted by "Christof Paar", https://www.youtube.com/watch?v=TTNtp9c3vKI (accessed 31 Oct. 2025). See time -8:55 (1h 5min 8sec) for the discussion on Salsa20.

[8] Cryptopals. "The Cryptopals Crypto Challenges." Available at: https://cryptopals.com/ (Accessed: October 22, 2025).

[9] Daniel J. Bernstein et al. "NaCl: Networking and Cryptography Library." Available at: https://nacl.cr.yp.to/stream.html (Accessed: October 31, 2025).

[10] Crypto++ Team. "Salsa20." Crypto++ Wiki. Available at: https://www.cryptopp.com/wiki/Salsa20 (Accessed: October 31, 2025).

[11] Libsodium Documentation. "Salsa20 Stream Cipher." Available at: https://libsodium.gitbook.io/doc/advanced/stream_ciphers/salsa20 (Accessed: October 31, 2025).

[12] System Weakness. "Understanding Salsa20 Encryption: A Comprehensive Guide." Published February 22, 2023. Available at: https://systemweakness.com/understanding-salsa20-encryption-a-comprehensive-guide-2023-2d6688889e4 (Accessed: October 31, 2025).

[13] Wikipedia contributors. "ChaCha20-Poly1305." *Wikipedia, The Free Encyclopedia*. Available at: https://en.wikipedia.org/wiki/ChaCha20-Poly1305. Accessed November 1, 2025.

[14] Arka Rai Choudhuri and Subhamoy Maitra. "Differential Cryptanalysis of Salsa and ChaCha – An Evaluation with a Hybrid Model." Available at: https://eprint.iacr.org/2016/377.pdf. Accessed November 1, 2025.