# Write a critique on one of the following papers:

- Adrian, David, et al. “Imperfect forward secrecy: How Diffie-Hellman fails in practice.” Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015.
- Text-only, about 1500+ words with lab will be plus.
  - 1 to 5 persons
- **Submit your Critigue by May 4, 2023 11:59 pm.**
-

https://blog.gslin.org/archives/tag/hellman/
https://rishabhjainnsit.wordpress.com/2018/11/01/paper-review-imperfect-forward-secrecy-how-diffie-hellman-fails-in-practice/

# Grading components

Critique should contain the following:

1. **Summary** – answering these four questions in your own words:
   - What problem is the paper trying to solve?
   - Why does the problem matter?
   - What is the approach used to solve the problem?
   - What is the conclusion drawn from this work?
2. **Strength(s) of the paper**
3. **Weakness(es) of the paper**
4. **Your own reflection, which can include but not limited to:**
   - What did you learn from this paper?
   - How would you improve or extend the work if you were the author?
   - What are the unsolved questions that you want to investigate?
   - What are the broader impacts of this proposed technology?
5. **Realization of a technical specification or algorithm as a program extra credit.**