Making the Presentation

* Utilize the LaTeX Package Beamer
* Some graphics from the paper itself can be reused
* Others will have to be simplified due to time constraints

Themes

* I will attempt to touch on the more generally interesting, less mathematically heavy segments of the paper 🡪 a greater focus will probably be placed on chapter 3
* OTP can be explained rather easily without going into the more complex mathematical side (e.g proof of secrecy)
* AES will be explained using the “general structure” of AES while still highlighting some of the key points in regards to the actual math behind the algorithm
  + First the general structure
  + Each of the four main steps can be explained in rather simple terms
  + Key expansions and finding the multiplicative inverse will have to be defined at some point before this
* The interesting aspects of the third chapter definitely fit better into a presentation than the heavier, more mathematical side of the paper
  + The historical and current effect of cryptography on our lives 🡪 everyone uses a variety of systems nowadays, most without giving conscious thought to it
  + How Diffie-Hellman enabled the usage of AES over insecure channels 🡪 at the beginning, pose the “infinite encryption problem” (“why encrypt a message if you still need to send the key?”) 🡪 Diffie-Hellman can also be explained using the “paint-mixing method” while still touching on the mathematical side

Approximate time plan

* Total time allocated: ca. 25-30 minutes
* OTP: 7 minutes
* AES: 10 minutes
* Cryptography in society / history: 10-13 minutes
* I would like to have more time to speak on the third points, as I feel it will resonate more with the audience who have not intimately familiarized themselves with things like finite fields or modular arithmetic 🡪 will attempt to shave off some time of the first two points in order to also include the relevance of cryptography in the historical development of computers