**Lab 10 Template – Ethan Roepke**

**Part 01**

1. **“outfile-Good text” pdf and “out-file Bad text” pdf (upload the files in canvas submission)** (10 points)
2. **Screenshot of the hashes of the text PDFs colliding for SHA1 and differing with SHA512** (10 points)
3. **Explain why the SHA1 hashes are the same for different files, but the SHA512 hashes are different.  Please be specific about how the near collision/collision works.** (10 points)
4. **Image out-1.pdf and Image out-2.pdf (Upload the files in canvas submission)** (10points)
5. **Screenshot of the hashes of the image PDFs colliding for SHA1 and differing with SHA512** (10 points)
6. **How likely is this to be used to carry out an attack in the wild?** (10 total points)

**Part 02**

1. **Upload your code to canvas as a separate .py file** (10 points)
2. **What is the winning lottery number for November 12th, 2024?** (5 points)
3. **In your own words, what is the seed for this random number generator? You must provide the correct values for both pieces used in the November 11th pull and explain the calculation made to earn full points.    Why is this a good or bad thing?** **Justify your answer.** (15 total points)
4. **What would be an alternate way to seed this random number generator such that it couldn’t be predicted either forward or backward?**  **Justify your answer.**

(10 total points)