ITP 125 Lab 6

1. It is used as a pseudorandom “mixing” function by the Random Number Generator and by the header key derivation function.
2. The randomness of the mouse moving creates a non-well-known seed for the random generator to produce numbers truly random
3. I’m not sure how I feel about these laws and it reminds me of when Apple had to produce the “key” to cracking the code to the terrorist iPhone used in San Bernardino and Apple declined. On one end I understand that it helps fight against terrorism but on the other Apple has a right to their information to protect its customers. I’m not really sure I understand how any company or service can get around laws like this in countries have implemented such laws.
4. The United States protects anyone from being forced to incriminate themselves. Currently in the U.S., there is no law regarding key disclosure.
5. I think the best way to get the passwords to the grader would be to also encrypt the passwords in a key that only the student and grader share but then again I’m not sure how that would happen entirely. Funny how this works.
6. Considering its safety was compromised, it clearly doesn’t seem safe to use anymore and I don’t think users would have truly protected information using it. I don’t know enough about these services or truly how they work to know what other alternatives there are but through this process of trying to get my homework submitted, I feel as though Veracrypt is safe. But then again, I could be wrong.