**ITP 125 - Lab 6**

**Tanuja Mohan**

**Questions**

1. I believe that Veracrypt needs a hashing algorithm in order to keep this key hidden so that not just anyone can access the information. Symmetric encryption uses one key to encrypt and decrypt and for this reason it is important to keep the key hidden and transfer it securely. By using a hashing algorithm, we are hiding the key and keeping it safe from those who we do not want to have access to the information.
2. The randomness generated from moving our mouse around allows us to generate a random key. This technique prevents any pattern from emerging in the random keys. No person can recreate the random movements of the mouse because even the slightest different produces a different value. In this way, all the keys are purely random and are always unique.
3. I think that Veracrypt is circumventing this law by keeping all the keys as the company’s private property rather than the user’s property. This way if legislation needs access to an individual’s information, the government would need to issue a warrant to Veracrypt rather than issue the warrant to the user. The government would need to show reasonable cause for why a warrant is needed against Veracrypt which is more difficult than proving that a warrant is needed against an individual. I understand why these laws are in place because if someone’s private property is directly affecting someone else’s then the government should have access to it. I understand only in the cases where someone else’s privacy/rights are being violated.
4. In the United States, passwords and encryption keys are classified as “knowledge” meaning that the fifth amendment protects citizens against incriminating testimonies. In other words, the constitution protects people from having to tell their passwords and encryption keys. Therefore, if I were to get stopped by security at an airport and if security were to demand my password, I would not need to tell them because I am protected by my fifth amendment.
5. I plan on telling the graders personally what my homework key is. This way, I can personally ensure that no one else overhears the key or that another person is present to hear the key. I could write the key on a piece of paper and show it to my grader so this way no can over hear it. Then, once the grader has entered the key into the homework I can shred the piece of paper so that no one else will be able to see it. This method ensures that the grader has to open the file right there in my presence or at least saves the key in a secure location so that it can’t get compromised on his/her end.
6. Based on the readings, I do not believe TrueCrypt is safe to use. This is because if TrueCrypt’s creators shut it down without any clear announcement of why they were doing so then this immediately makes me suspicious that the reason for the shutdown is something that would make the public concerned or mad about. The articles also mentioned that the website displayed a warning message to all of its users. There is a suspicion that someone simply hacked into the website and displayed the error message, but the fact that someone could hack into the website makes users believe that if the hackers could hack into the website then they could hack into their documents as well. After browsing online I have found some alternatives that have high reviews such as cypherix encryption software. This software has great reviews and is widely used by companies with the companies giving no complaints as of yet. Since there is such a large user base and little complaints this makes me feel as though this is a great alternative to VeraCrypt.