Questions

1. In step 5 of the lab, you could choose a different hashing algorithm for the encryption. We will talk about hashing later on, but if we’re doing symmetric encryption why does Veracrypt need a hashing algorithm?

Curiosity is your friend.

**This allows the program to turn the password into a secure code that is safe to store**

1. In step 8, the program asked for you to move the mouse around. What is the point of randomness generated from this? How is it used in the encryption?

**It is hard to emulate randomness in a computer as it can always be replicated again. Even using the clock is not random enough. However it is difficult to emulate the exact same mouse movement, thus this is used to for randomness.**

1. Certain countries have a [Key disclosure laws](http://en.wikipedia.org/wiki/Key_disclosure_law). How do you think Veracrypt can help circumvent the law that is in place? Do you agree with these laws? Explain.

**Yes, since security will not go as far as checking for hidden volumes. I believe that your personal files are effectively the same as your personal belongings. If you’re going to hide things you don’t want others seeing, you’ll hide them in a secret compartment physically. Same with digital information. Authorities should have access to your belongings (like searching your home for stuff), but if you really need to hide stuff, then you should hide stuff well.**

1. In the previous question, we talked about Key disclosure laws. How does the US handle the disclosure of passwords? If you were crossing airports and security officials demanded your password, do you have to?

**I don’t think the US has this law. Or at least I haven’t come across it.**

1. In order to submit this lab, you will need to place the answers to this lab into a Veracrypt volume that is not more then 250KB. You may use any password(s) that you like.

How do you plan to get the password to the volume to the grader securely?

**You can always meet up with them during their grading sessions and communicate the password through discrete methods (writing it down on a piece of paper away from other’s view, and show it to the grader, then destroy the paper).**

If you plan to place the password in the email what’s the point of encryption if anyone can read it. Think about the best way possible without leaking the password to anyone (even the email servers). Only you and the grader should know the key.

**Indicate which letters constitutes your password by index numbers of your email, then give it to your grader.**

1. Read the some of the following articles:

<https://isc.sans.edu/forums/diary/True+Crypt+Compromised+Removed/18177/>

<http://www.tomsguide.com/us/Truecrypt-may-be-compromised,news-18861.html>

[http://krebsonsecurity.com/2014/05/true-goodbye-using-Veracrypt-is-not-secure/](http://krebsonsecurity.com/2014/05/true-goodbye-using-truecrypt-is-not-secure/)

Based on your readings, do you still think Truecyrpt is still safe to use? Explain. Can you think of any alternatives to Veracrypt that you would trust using?

**For security related matieral, the developer / organization who maintains this should be transparent. I’ll need to look up Veracrypt to see how transparent they are.**