DFSC1316: Digital Forensic and Information Assurance I

Assignment 2 (Due Tue, 10/24/2017 23:59:99)

Rules:

1. All you answers will be typed unless otherwise being advised.
2. Submit you assignment in PDF version (Office word can be directly saved as PDF, or you can use virtual PDF printer to 'print' it as pdf).

---

1. (25pts) What is the main difference between secret key cryptography algorithm and public key cryptography algorithm? Explain why secret key algorithm does not support non-repudiation, and how can public key algorithm support it.

2. (25pts) Explain how to implementation authentication between Alice and Bob, using secret key, public key, and Hash algorithms.

3. (25pts) Why it is so important that we require it is difficult to find two messages with the same message digest?

4. (25pts) Bob obtained a forensics copy (that is, an image) of a hard drive from a crime scene. He runs a Hash algorithm to compute the Hash of the image, and stores the Hash value along with the image on a portable hard drive, which is then taken care of by Trudy.
   After some time, when Bob get the hard drive back from Trudy, he suspect that Trudy may have changed the content of the forensics image.
   Therefore, Bob run the same Hash algorithm again with the image on the hard drive, and found that the Hash value matches what was stored on the hard drive.
   Question: is this an indication that Trudy has not done anything to the image? Why or why not?