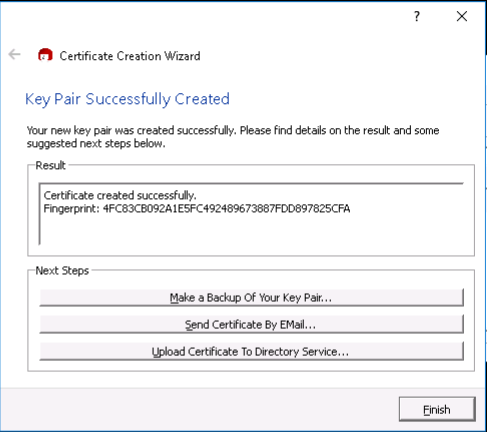
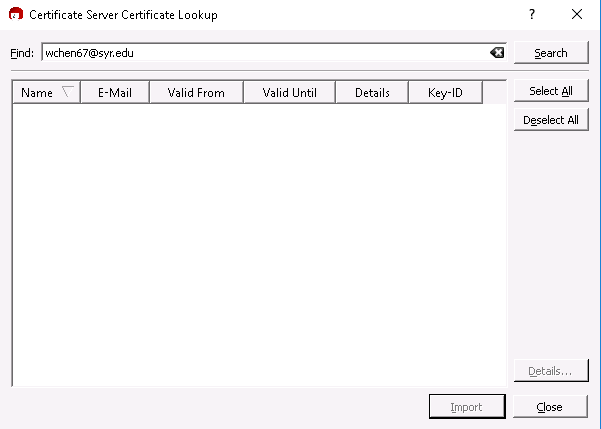
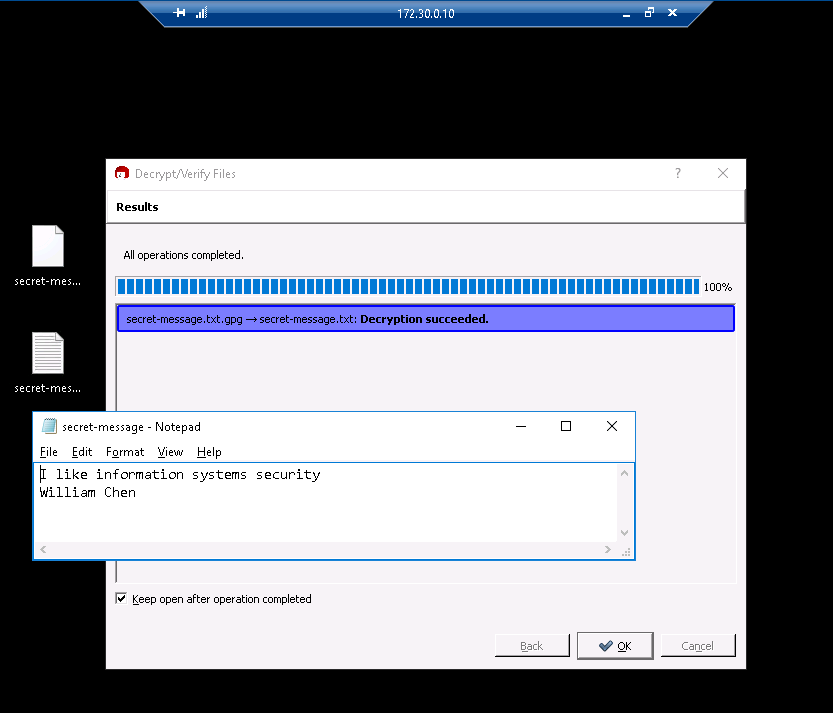
William Chen IST 323 – M002

Professor Christopher Croad 09/22/2020

Lab #2 - Using Encryption to Enhance Confidentiality and Integrity

1. **Part One, Step #11: Generated Fingerprint**
2. **Part One, Step #17: Certificate Server Certificate Lookup (certificate wasn’t able to upload so it’s empty)**
3. **Part Four, Step #22: Kleopatra Decryption Results Window** 
4. **Part 5: Challenge Question, What is the difference between X.509 and PGP certificate types?**
   1. A certificate authority issues X.509 certificates, usually used for websites and PGP certificates can be used by anyone and usually used to encrypt files and emails. An example of an X.509 certificate authorizer is Verisign. Many people trust Verisign, and its key is built into browsers. An example of a site that uses X.509 or, more specifically, Verisign’s certification is Amazon. The browser knows Verisign’s key, and since Verisign signs Amazon’s key, we can trust Amazon’s key is Amazon. Meanwhile, PGP is based on whether you want to trust someone or not. For example, I would have to check whether a key belongs to someone manually. If someone tells me their key, it would be up to me to determine whether the key is genuinely theirs or if it was someone else. Anyone can create a PGP key, but not anyone can have an X.509 key. It must be assigned by a trusted certificate authority such as Verisign.