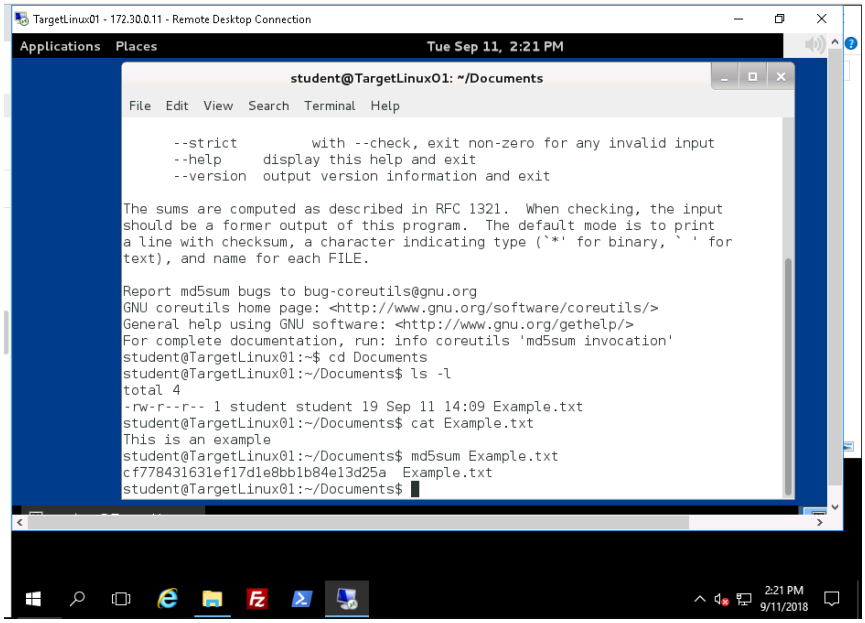
MARYMOUNT UNIVERSITY

Assignment: IT557; Monitoring, Auditing, and Penetration Testing
Assigned: Sep. 16, 2018
Instructor: Professor Ali Bicak
Student Name: George Boakye

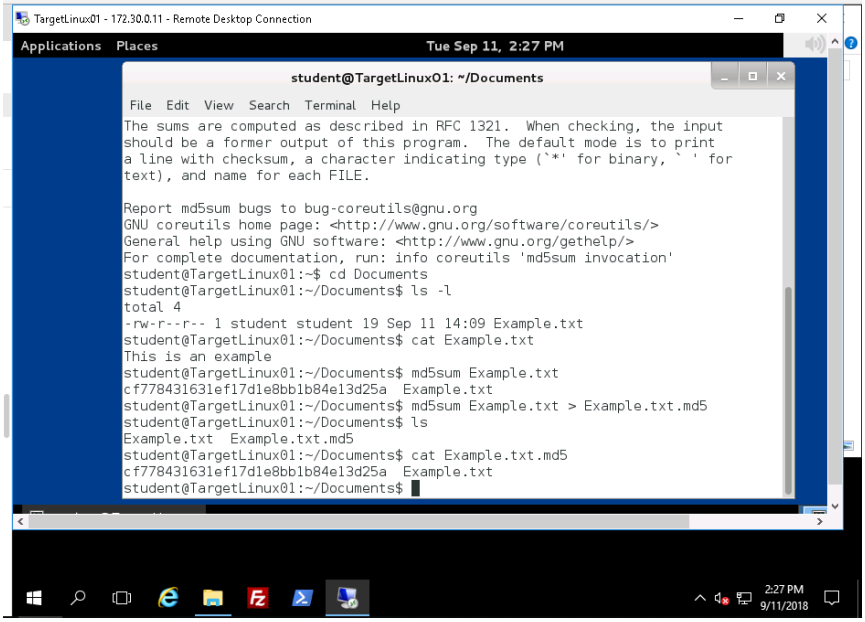
LAB REPORT FILE (LAB2)

SECTION 1

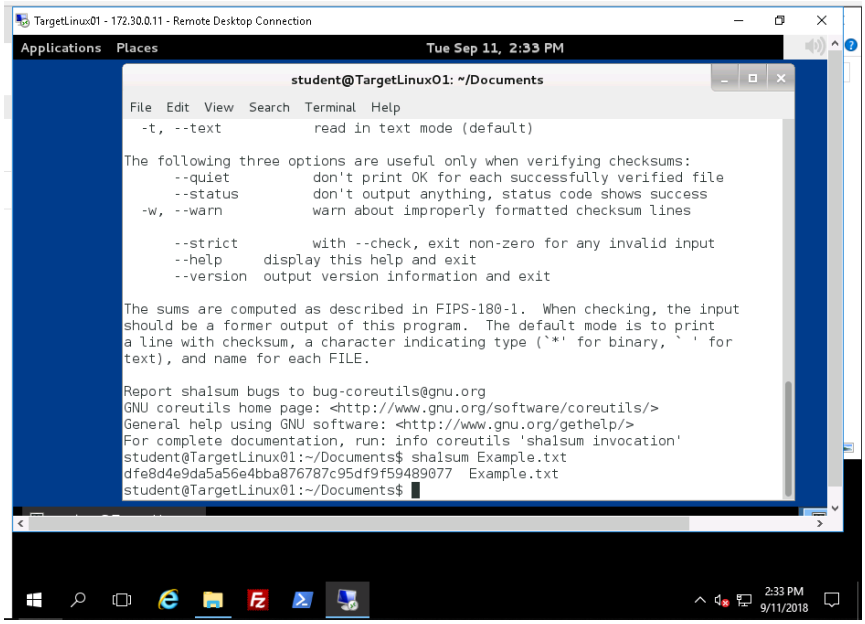
Part 2: Step7: md5 hash Output



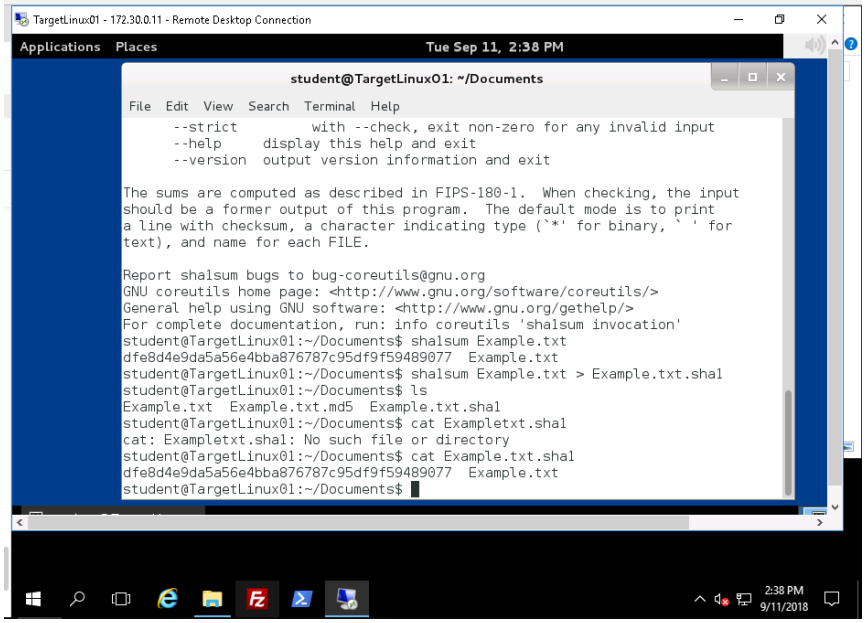
Part 2: Step11: Example.txt.md5 Output



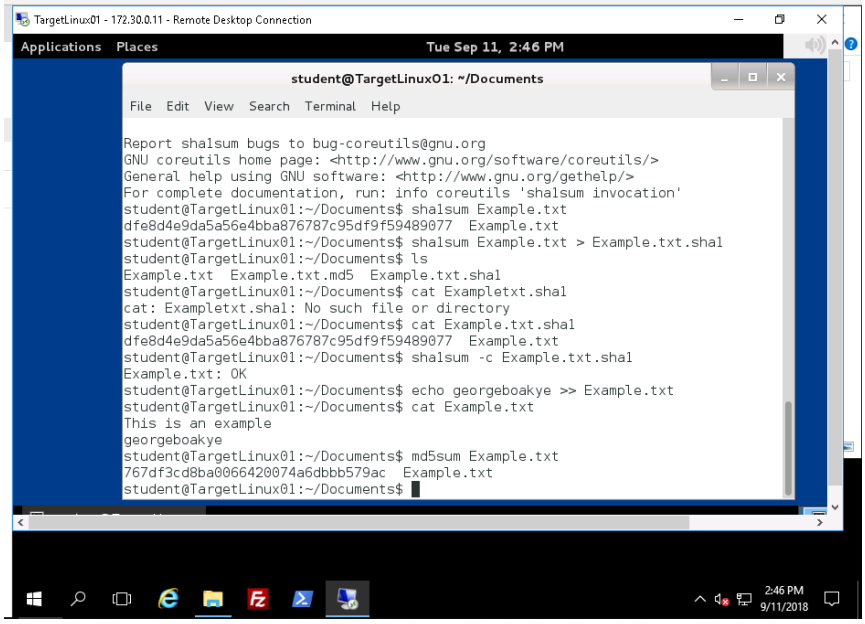
Part 2: Step15: sha1sum hash for Example.txt Output



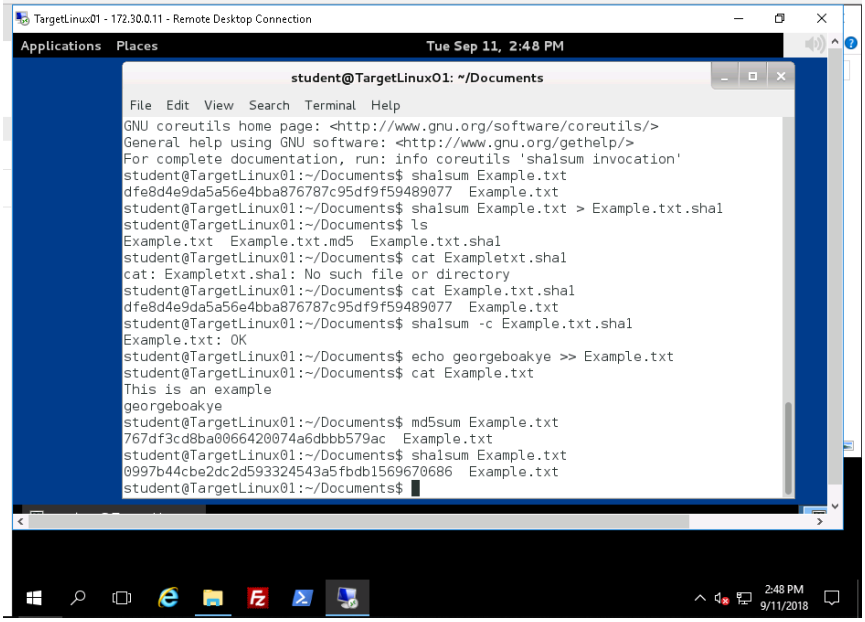
Part 2: Step19: Example.txt.sha1 Output



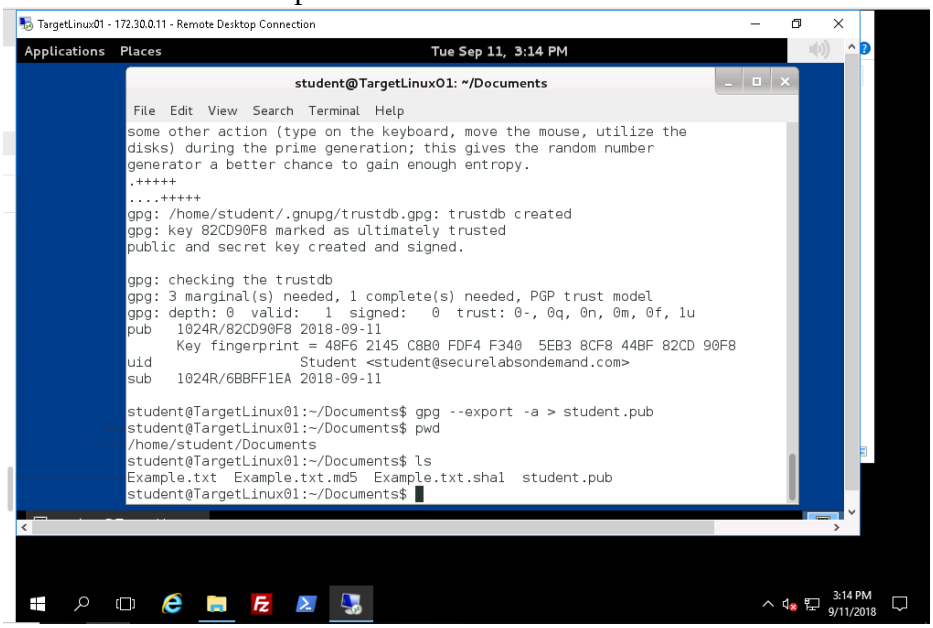
Part 3: Step4: New md5 hash Output



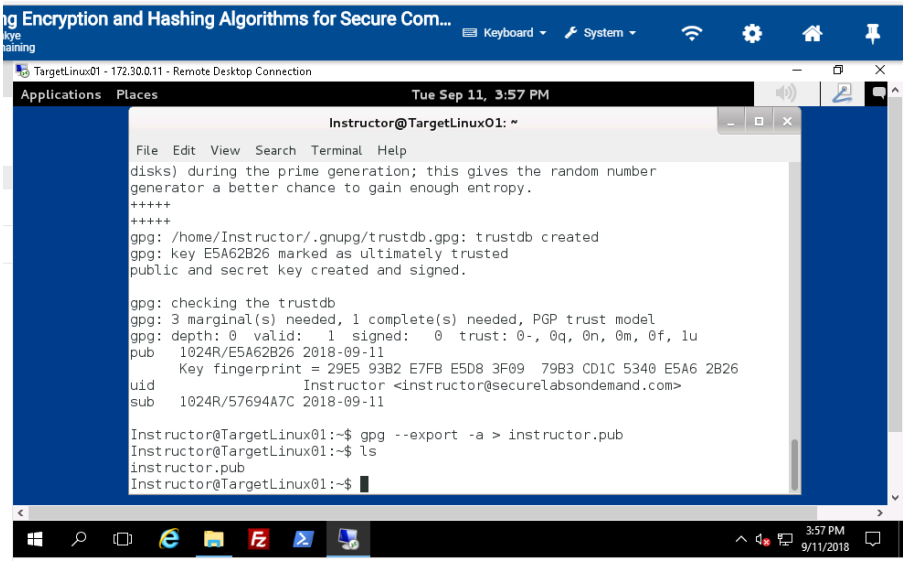
Part 3: Step6: New sha1 hash Output



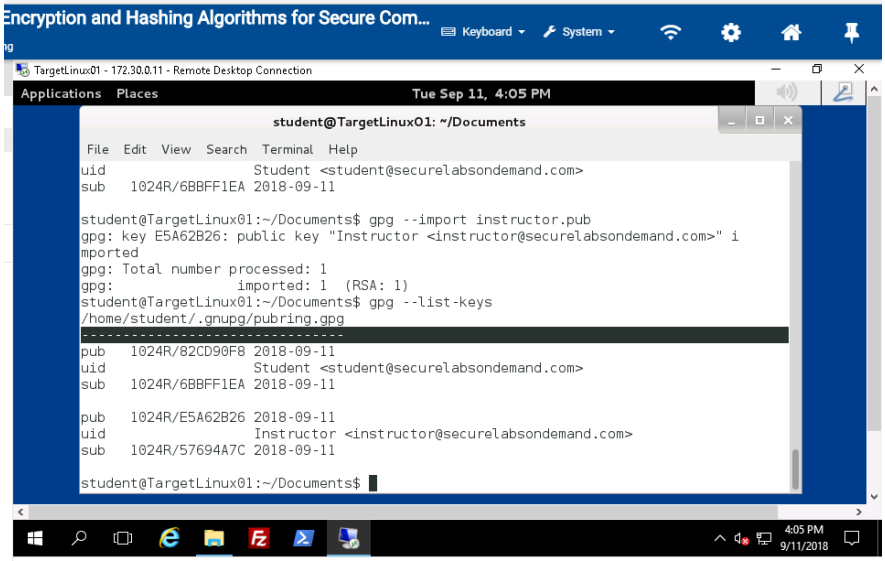
Part 4: Step13: /home/student/documents folder



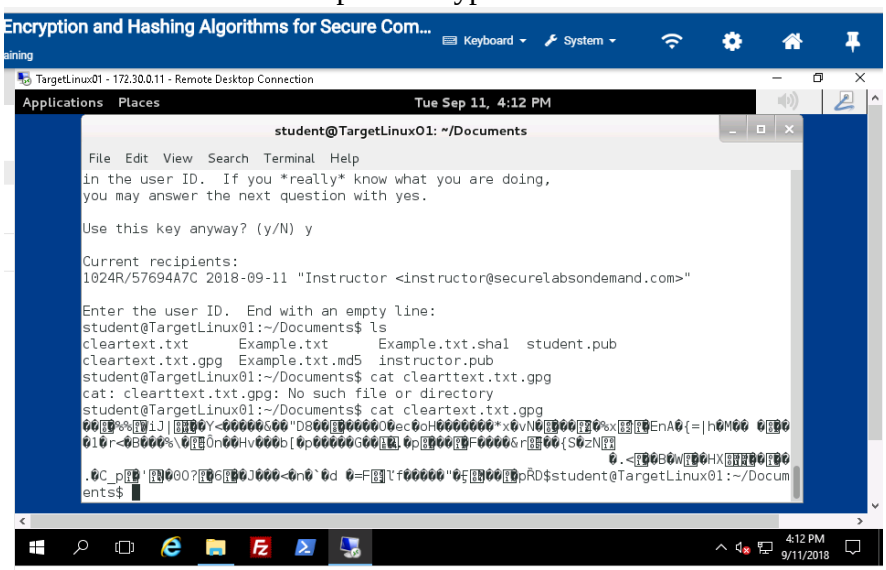
Part 4: Step 21: instructor folder



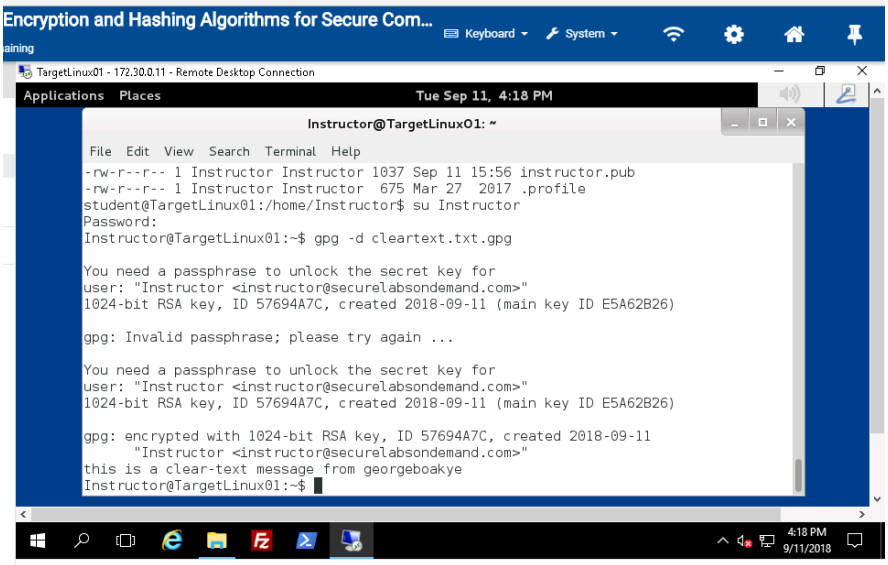
Part 5: Step 6: Exchange PGP Keys



Part 6: Step 8: Encrypted cleartext.txt

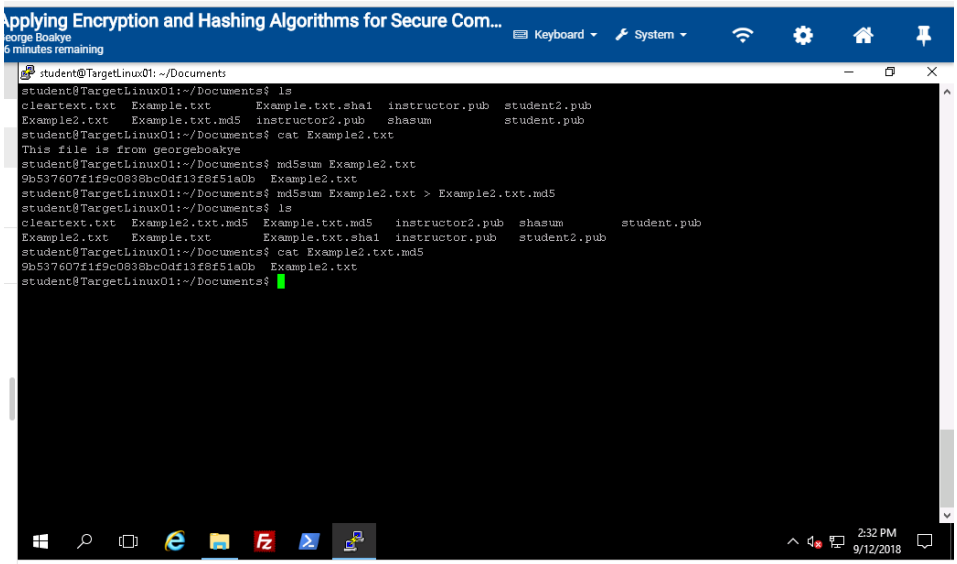


Part 6: Step 19: Decrypted cleartext.txt message

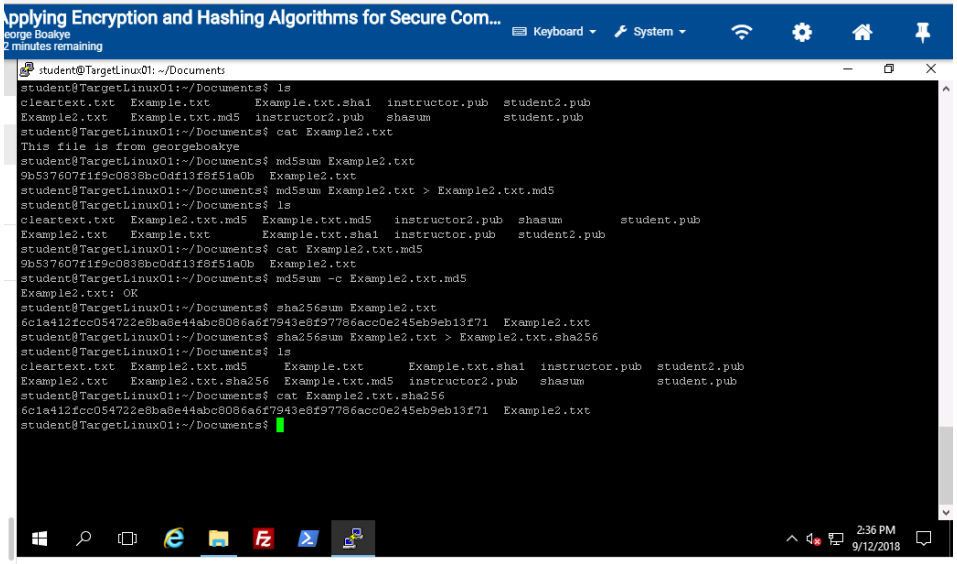


SECTION 2

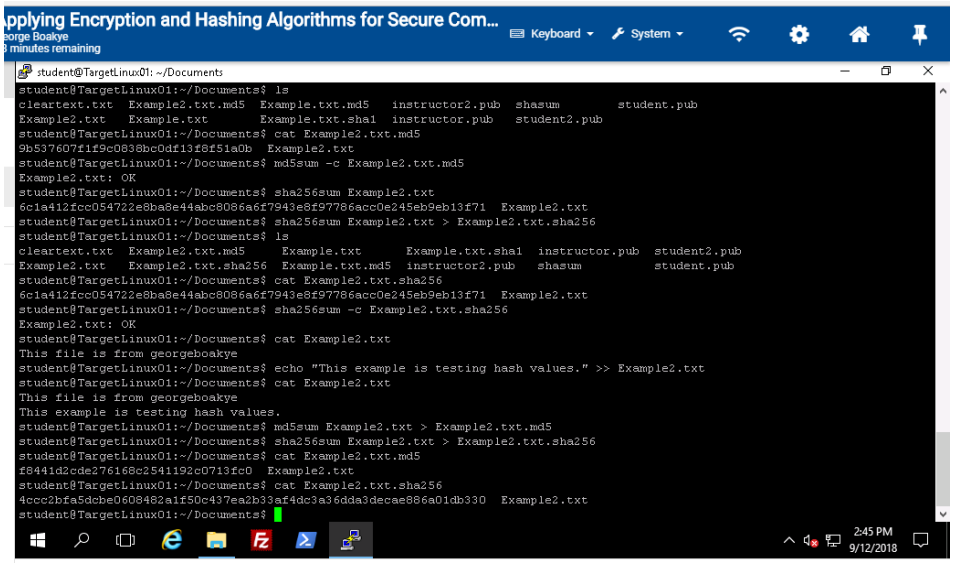
Part 2: Step 6: Example2.txt.md5



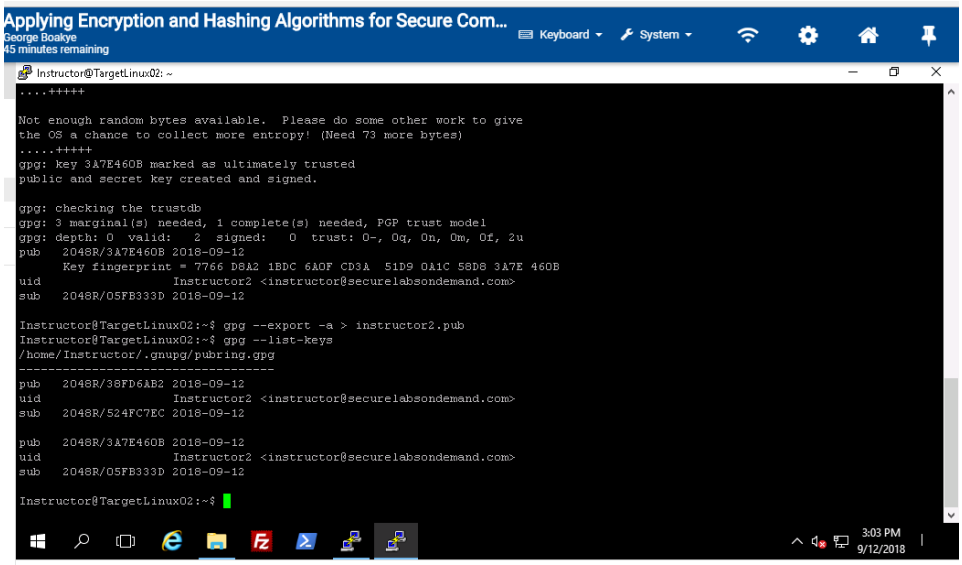
Part 2: Step 14: Example2.txt.sha256



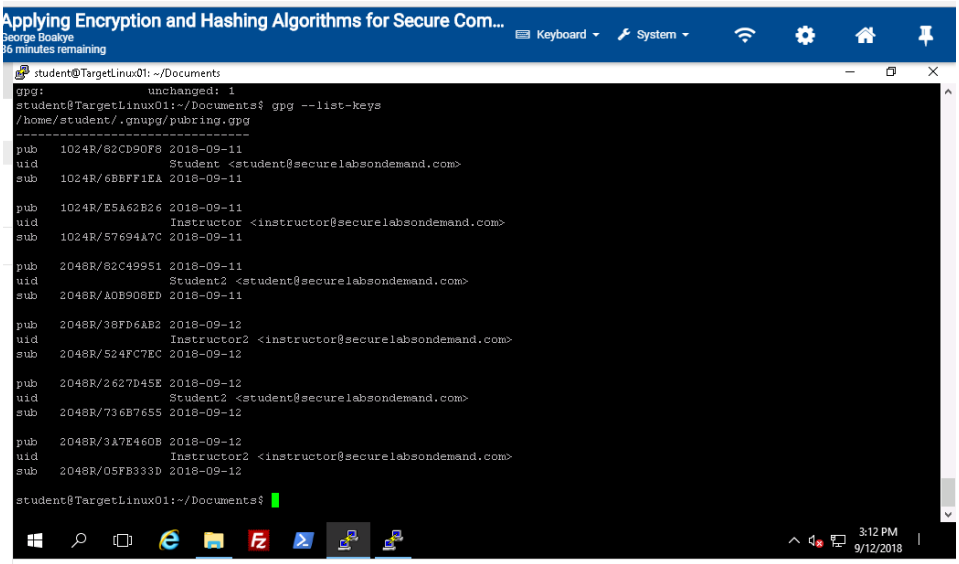
Part 3: Step 7: Modified MD5suma and SHA256 hash



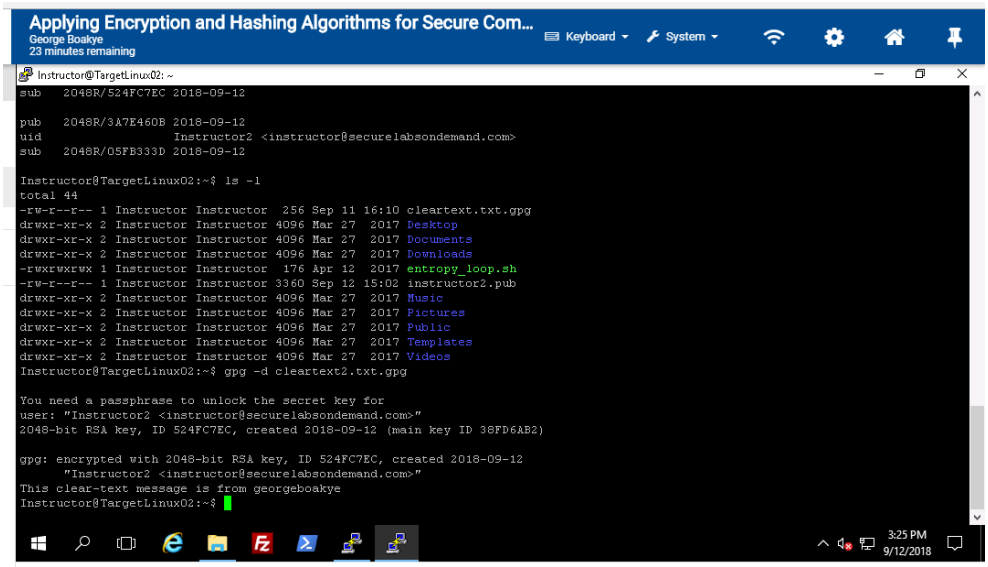
Part 4: Step 17: Instructor's public key ring



Part 5: Step 12: Updated student's public key ring



Part 6: Step 19: Instructor decrypts message



SECTION 3

Part 1

Differences between RSA and ECDSA encryption algorithms. Product that uses each type of encryption.

RSA and ECDSA are algorithms used by Asymmetric (public key) cryptographic systems to provide a mechanism for authentication (collectively called digital signature algorithms). They are mathematical problems that are complex and relatively simple to compute one way but impractical to reverse. Some ECDSA products are iPhone and iPad (Genkin, Pachmanov, & Pipman, 2016). RSA products include RSA SecureID Tokens, USB Flash Drives, and Smart Cards (RSA SecurID, 2018).

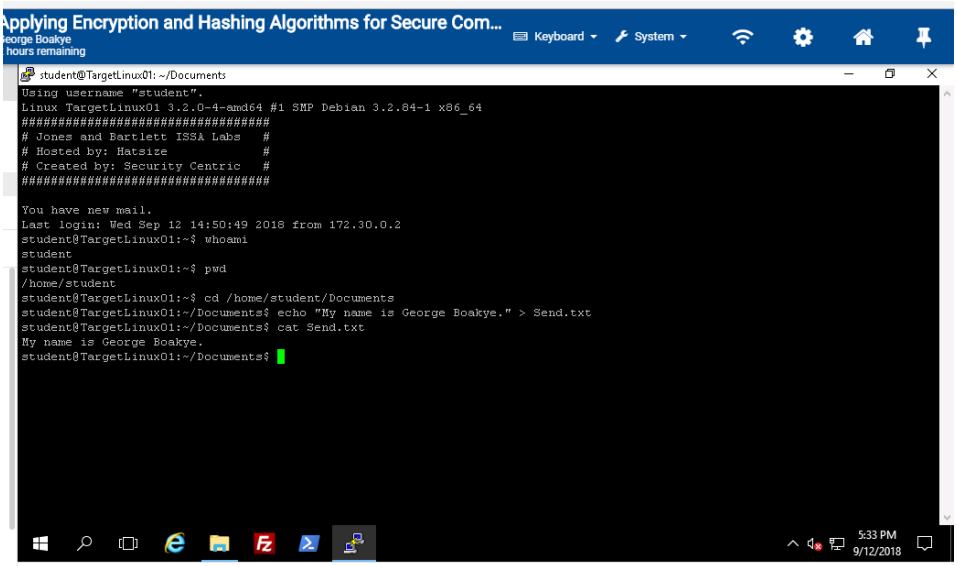
Here are the key differences (Naziridis, 2018):

Standard maturity: RSA was first standardized for SSL/TLS in 1994, while ECDSA was introduced in the specification of TLS v1.2 in 2008. This makes RSA extremely recognized and more used than ECDSA.

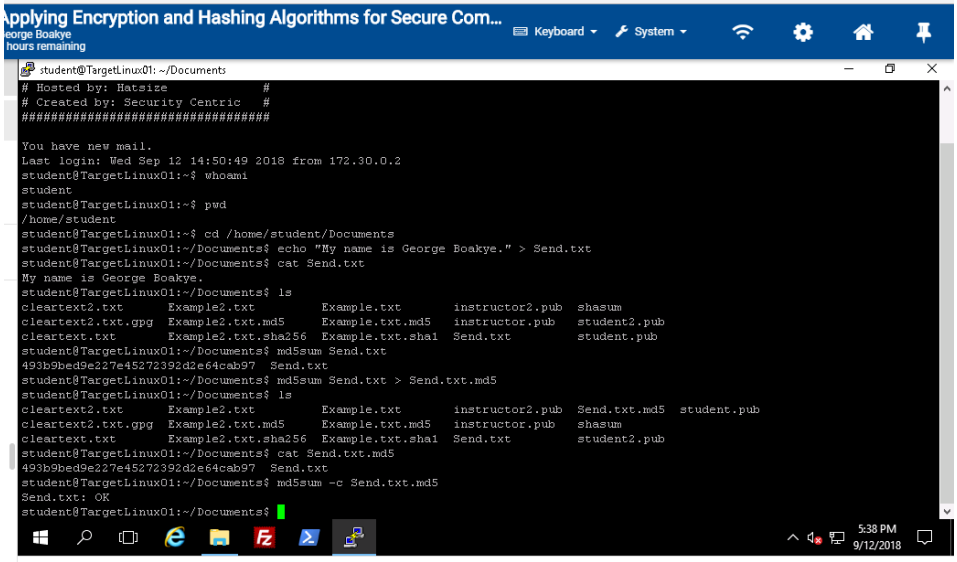
Key-size to security-level ratio: An RSA 2048-bit public key provides 112 bits security level bits whiles ECDSA requires only 224-bit sized public keys to provide same 112-bit security level. The implication is smaller key sizes such as ECDSA (224-bit) require less bandwidth to set up an SSL/TLS stream. This makes ECDSA certificates ideal for mobile applications.

Performance & time complexity: During implementations, RSA seems to be significantly faster than ECDSA in verifying signatures but slower in message signing.

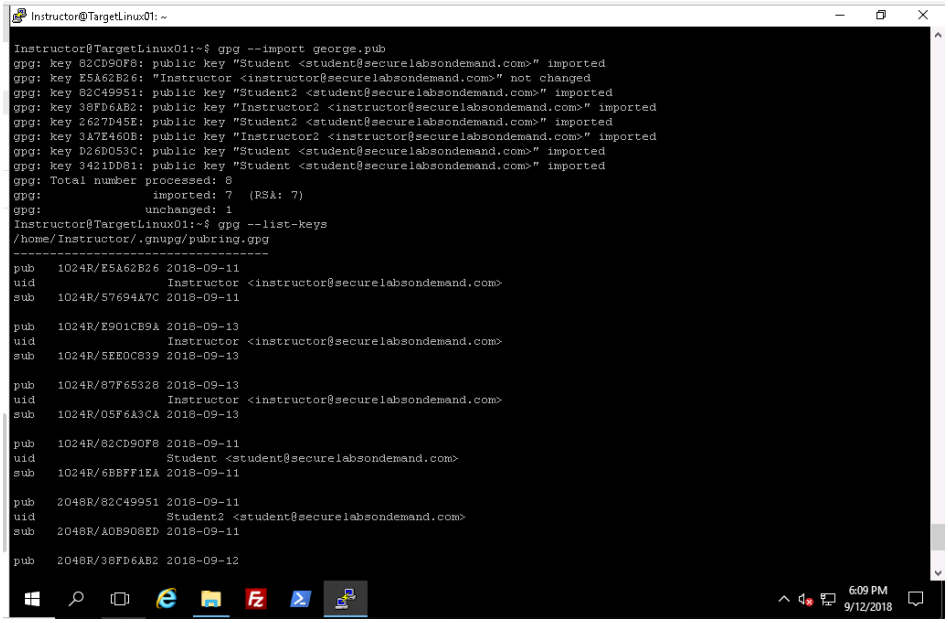
Part 2: A: Send.txt folder



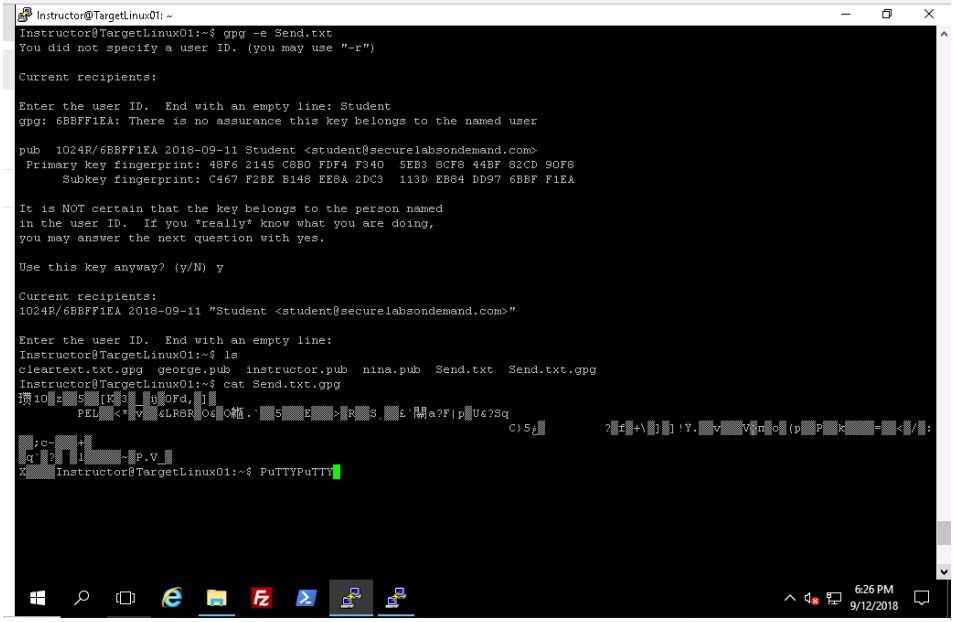
Part 2: B: MD5 hash for Send.txt



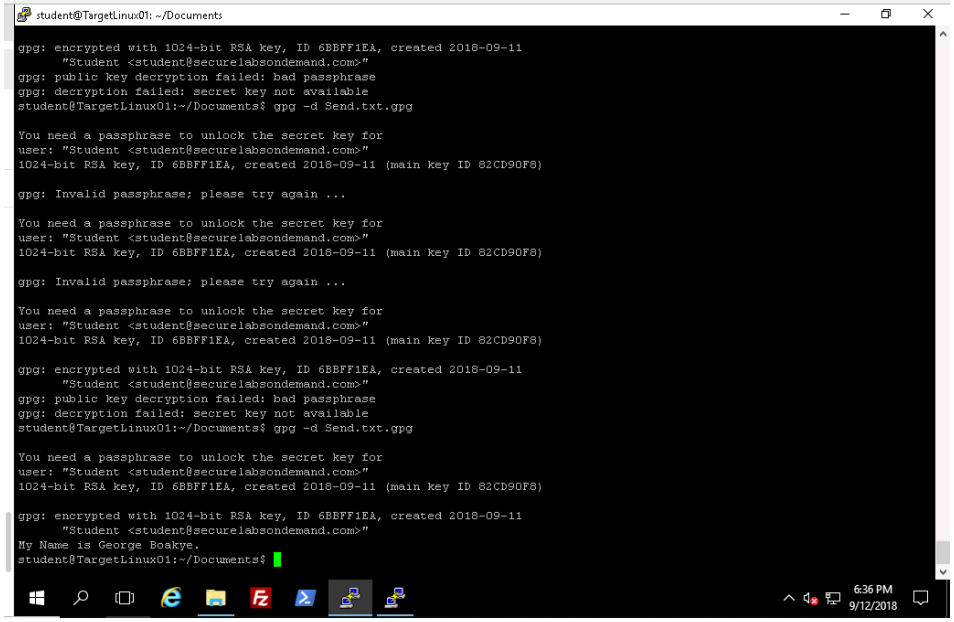
Part 2: C: Shared Student public key with Instructor



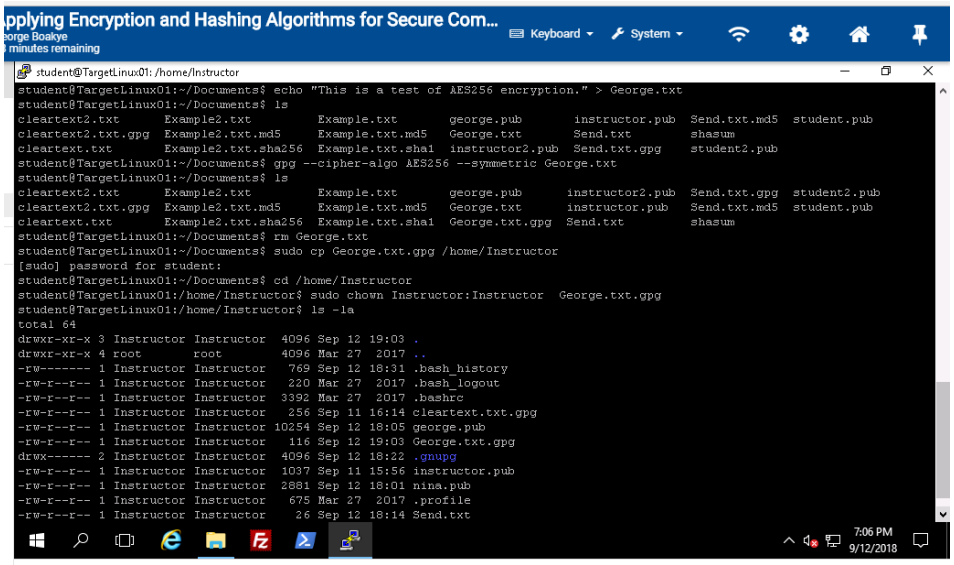
Part 2: D: Encrypting Send.txt with Instructor Account



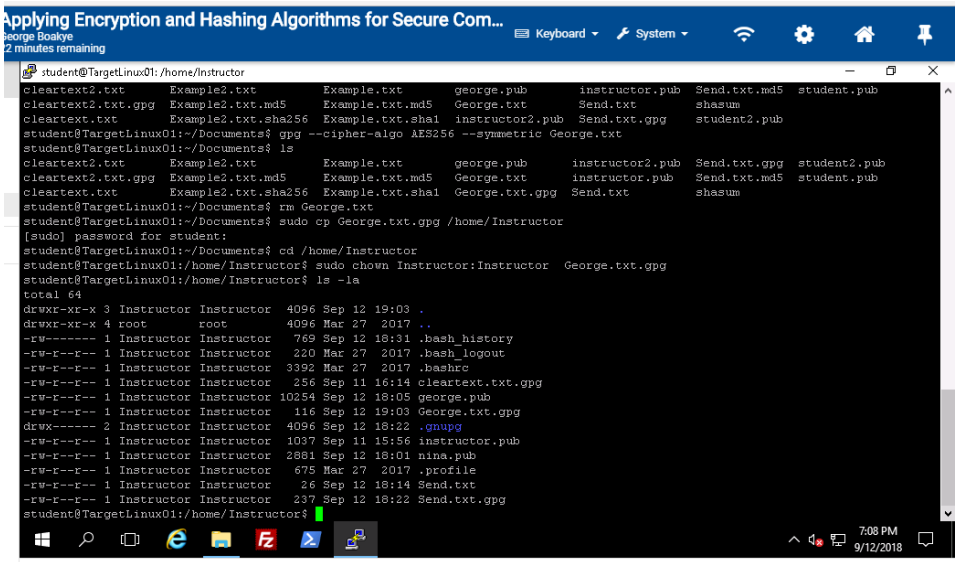
Part 2: E: Decrypting Send.txt.gpg with Student Account



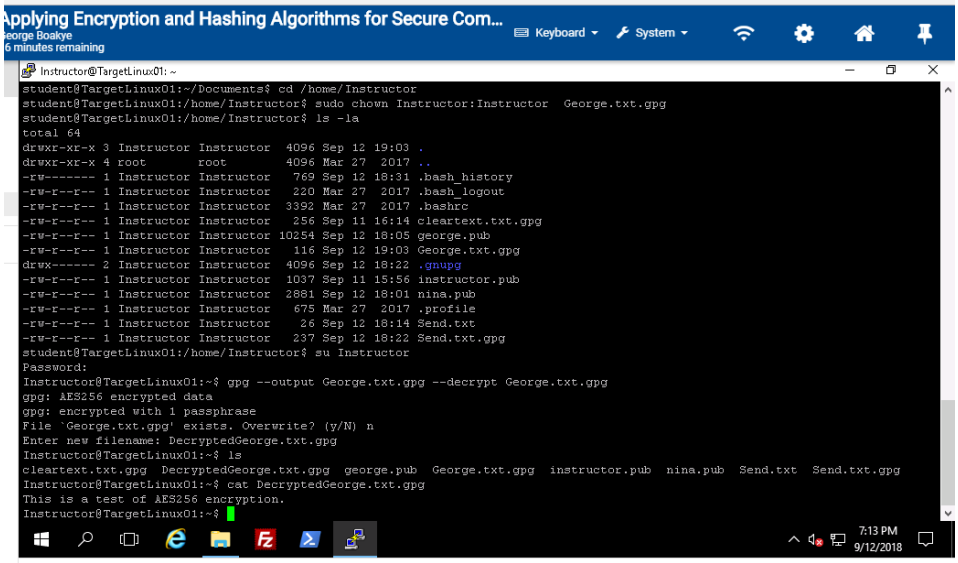
Part 3: A: George.txt created



Part 3: B: AES256 encryption method used



Part 3: C: Copied to Instructor Account, Changed Permission, & Decrypted



Reference

ask ubuntu. (2018, September 13). Retrieved from ask ubuntu: https://askubuntu.com/questions/60712/how-do-i-quickly-encrypt-a-file-with-aes

Genkin, D., Pachmanov, L., & Pipman, I. (2016, August 18). *ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels*. Retrieved from https://eprint.iacr.org/2016/230.pdf

Naziridis, N. (2018, June 27). *Comparing ECDSA vs RSA*. Retrieved from SSL.com: https://www.ssl.com/article/comparing-ecdsa-vs-rsa/

RSA SecurID. (2018, September 2). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/RSA_SecurID