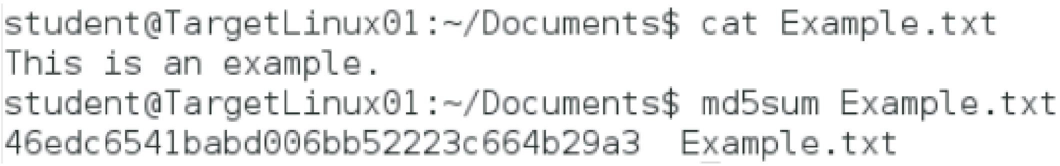
Lab 2: CEN4088.01 Due 9/26/2019

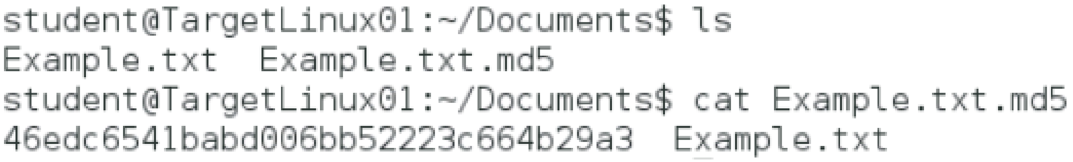
Brandon Thompson: 5517

September 26, 2019



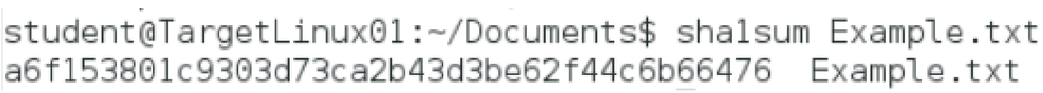
```
student@TargetLinux01:~/Documents$ cat Example.txt
This is an example.
student@TargetLinux01:~/Documents$ md5sum Example.txt
46edc6541babd006bb52223c664b29a3  Example.txt
```

Figure 1: MD5sum hash string for Example.txt.



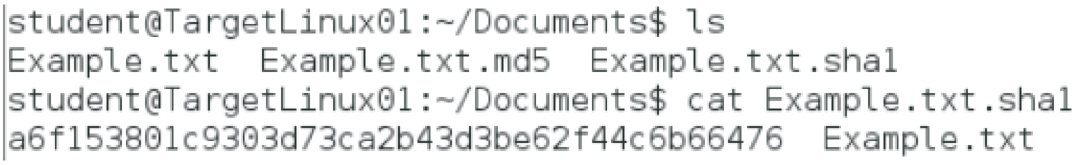
```
student@TargetLinux01:~/Documents$ ls
Example.txt  Example.txt.md5
student@TargetLinux01:~/Documents$ cat Example.txt.md5
46edc6541babd006bb52223c664b29a3  Example.txt
```

Figure 2: Contents of Example.txt.md5 file.



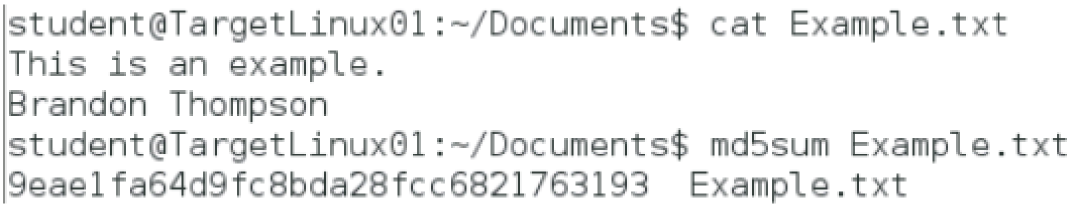
```
student@TargetLinux01:~/Documents$ sha1sum Example.txt
a6f153801c9303d73ca2b43d3be62f44c6b66476  Example.txt
```

Figure 3: SHA1sum hash string for Example.txt.



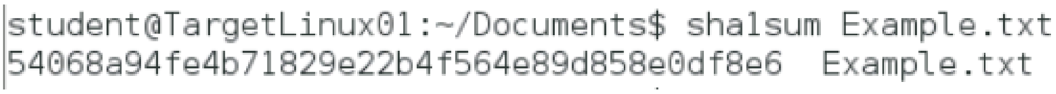
```
student@TargetLinux01:~/Documents$ ls
Example.txt  Example.txt.md5  Example.txt.sha1
student@TargetLinux01:~/Documents$ cat Example.txt.sha1
a6f153801c9303d73ca2b43d3be62f44c6b66476  Example.txt
```

Figure 4: Contents of Example.txt.sha1 file.



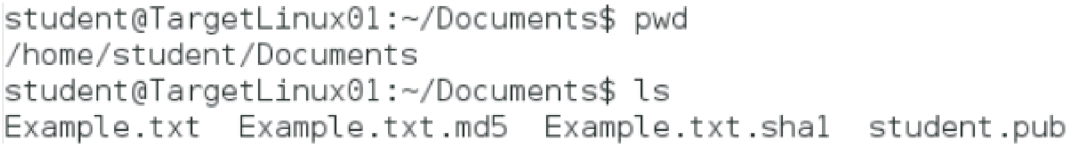
```
student@TargetLinux01:~/Documents$ cat Example.txt
This is an example.
Brandon Thompson
student@TargetLinux01:~/Documents$ md5sum Example.txt
9eae1fa64d9fc8bda28fcc6821763193  Example.txt
```

Figure 5: Modified MD5sum hash string.



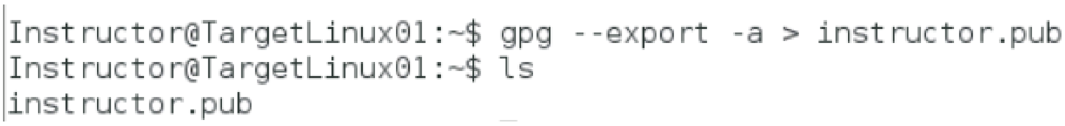
```
student@TargetLinux01:~/Documents$ sha1sum Example.txt
54068a94fe4b71829e22b4f564e89d858e0df8e6  Example.txt
```

Figure 6: Modified SHA1 hash string.



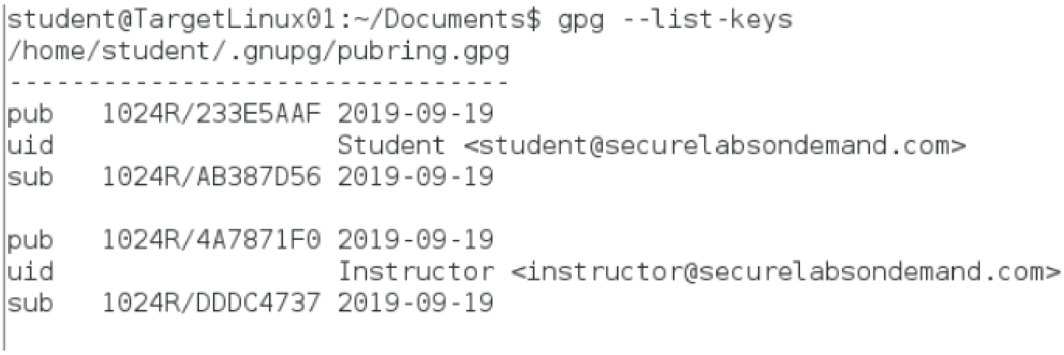
```
student@TargetLinux01:~/Documents$ pwd
/home/student/Documents
student@TargetLinux01:~/Documents$ ls
Example.txt  Example.txt.md5  Example.txt.sha1  student.pub
```

Figure 7: Contents of /home/student/Documents directory.



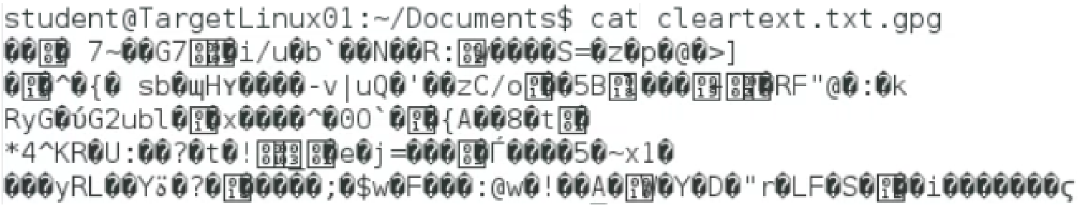
```
Instructor@TargetLinux01:~$ gpg --export -a > instructor.pub
Instructor@TargetLinux01:~$ ls
instructor.pub
```

Figure 8: Contents of /home/instructor directory.



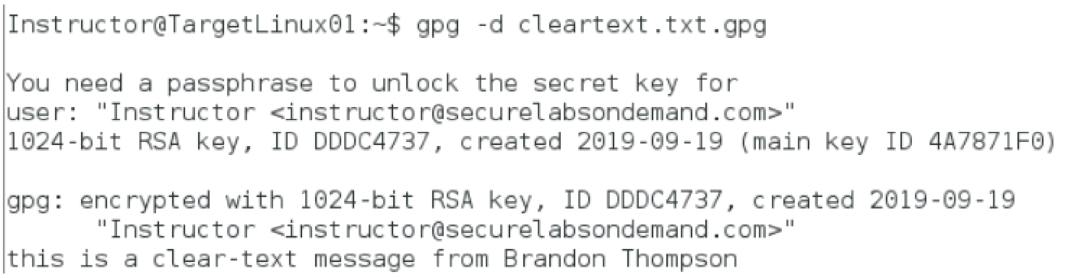
```
student@TargetLinux01:~/Documents$ gpg --list-keys
/home/student/.gnupg/pubring.gpg
--------------------------------
pub   1024R/233E5AAF 2019-09-19
uid                  Student <student@securelabsondemand.com>
sub   1024R/AB387D56 2019-09-19

pub   1024R/4A7871F0 2019-09-19
uid                  Instructor <instructor@securelabsondemand.com>
sub   1024R/DDDC4737 2019-09-19
```

Figure 9: List of strudent's public key ring.



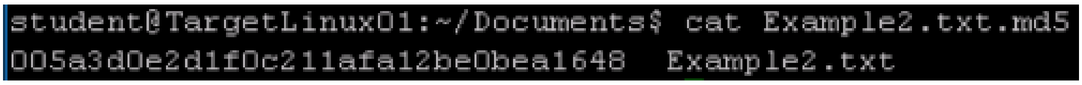
```
student@TargetLinux01:~/Documents$ cat cleartext.txt.gpg
��▯� 7~��G7▯▯�i/u�b`��N��R:▯�����S=�z�p�@�>]
�▯�^�{� sb�щHʏ����-v|uQ�'��zC/o▯��5B▯���▯▯�RF"@�:�k
RyG�úG2ubl�▯�x����^�0O`�▯�{A��8�t▯�
*4^KR�U:��?�t�!▯▯▯�e�j=���▯�Γ����5�~x1�
���yRL��Yӧ�?�▯�����;�$w�F���:@w�!��A�▯�Y�D�"r�LF�S�▯�i�������ς
```

Figure 10: Contents of encrypted cleartext.txt.gpg file.



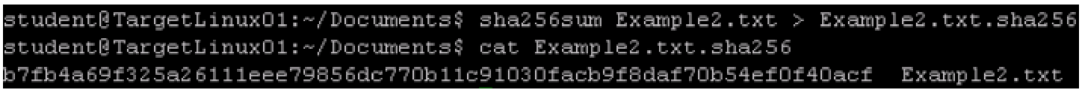
```
Instructor@TargetLinux01:~$ gpg -d cleartext.txt.gpg

You need a passphrase to unlock the secret key for
user: "Instructor <instructor@securelabsondemand.com>"
1024-bit RSA key, ID DDDC4737, created 2019-09-19 (main key ID 4A7871F0)

gpg: encrypted with 1024-bit RSA key, ID DDDC4737, created 2019-09-19
      "Instructor <instructor@securelabsondemand.com>"
this is a clear-text message from Brandon Thompson
```

Figure 11: Decrypted content of cleartext.txt.gpg file.



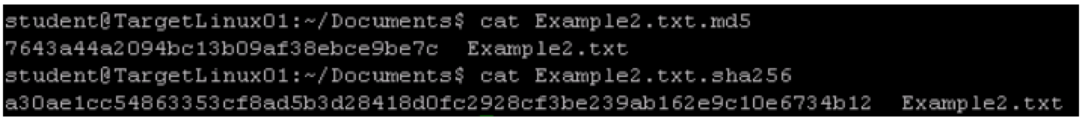
```
student@TargetLinux01:~/Documents$ cat Example2.txt.md5
005a3d0e2d1f0c211afa12be0bea1648  Example2.txt
```

Figure 12: Contents of Example.txt.md5 file.



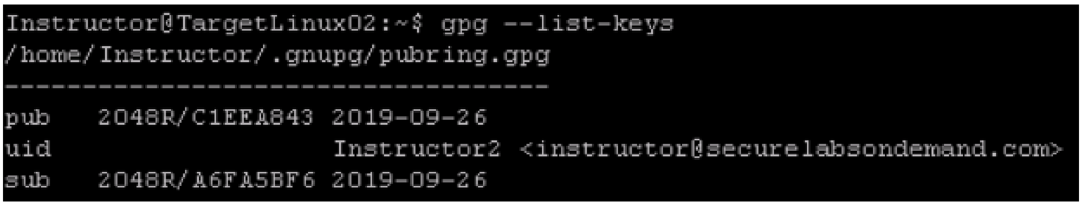
```
student@TargetLinux01:~/Documents$ sha256sum Example2.txt > Example2.txt.sha256
student@TargetLinux01:~/Documents$ cat Example2.txt.sha256
b7fb4a69f325a26111eee79856dc770b11c91030facb9f8daf70b54ef0f40acf  Example2.txt
```

Figure 13: Contents of Example2.txt.sha256 file.



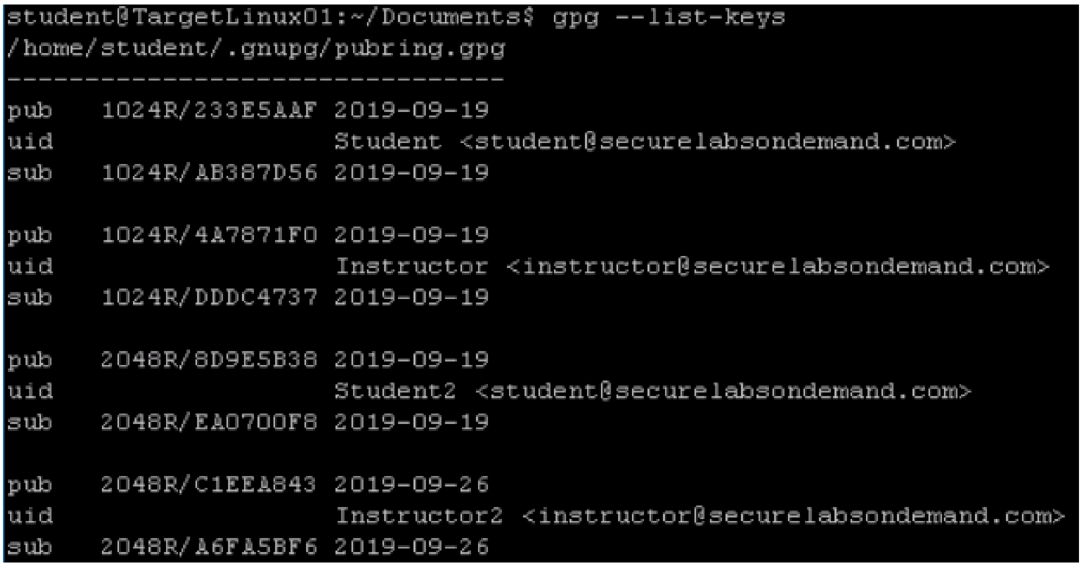
```
student@TargetLinux01:~/Documents$ cat Example2.txt.md5
7643a44a2094bc13b09af38ebce9be7c  Example2.txt
student@TargetLinux01:~/Documents$ cat Example2.txt.sha256
a30ae1cc54863353cf8ad5b3d28418d0fc2928cf3be239ab162e9c10e6734b12  Example2.txt
```

Figure 14: Modified MD5sum and SHA-256 hash strings.



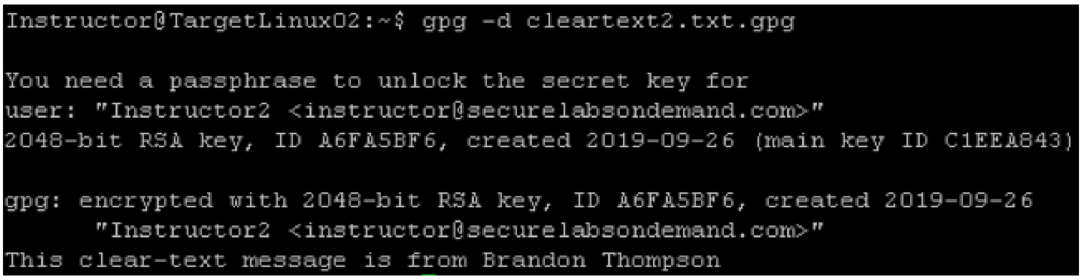
```
Instructor@TargetLinux02:~$ gpg --list-keys
/home/Instructor/.gnupg/pubring.gpg
-----------------------------------
pub   2048R/C1EEA843 2019-09-26
uid                  Instructor2 <instructor@securelabsondemand.com>
sub   2048R/A6FA5BF6 2019-09-26
```

Figure 15: Instructor's public key ring.



```
student@TargetLinux01:~/Documents$ gpg --list-keys
/home/student/.gnupg/pubring.gpg
--------------------------------
pub   1024R/233E5AAF 2019-09-19
uid                  Student <student@securelabsondemand.com>
sub   1024R/AB387D56 2019-09-19

pub   1024R/4A7871F0 2019-09-19
uid                  Instructor <instructor@securelabsondemand.com>
sub   1024R/DDDC4737 2019-09-19

pub   2048R/8D9E5B38 2019-09-19
uid                  Student2 <student@securelabsondemand.com>
sub   2048R/EA0700F8 2019-09-19

pub   2048R/C1EEA843 2019-09-26
uid                  Instructor2 <instructor@securelabsondemand.com>
sub   2048R/A6FA5BF6 2019-09-26
```

Figure 16: Student's public key ring.



```
Instructor@TargetLinux02:~$ gpg -d cleartext2.txt.gpg

You need a passphrase to unlock the secret key for
user: "Instructor2 <instructor@securelabsondemand.com>"
2048-bit RSA key, ID A6FA5BF6, created 2019-09-26 (main key ID C1EEA843)

gpg: encrypted with 2048-bit RSA key, ID A6FA5BF6, created 2019-09-26
      "Instructor2 <instructor@securelabsondemand.com>"
This clear-text message is from Brandon Thompson
```

Figure 17: Contents of decrypted cleartext2.txt.gpg.