Lab 04 Template

1) Part 1:
   a. **Screenshot of columnar output of all ciphersuites on Ubuntu 18.04 desktop** (10 points)

```
cpre331@desktop:~$  openssl ciphers -s -v
TLS_AES_256_GCM_SHA384  TLSv1.3 Kx=any      Au=any  Enc=AESGCM(256) Mac=AEAD
TLS_CHACHA20_POLY1305_SHA256 TLSv1.3 Kx=any      Au=any  Enc=CHACHA20/POLY1305(256) Mac=AEAD
TLS_AES_128_GCM_SHA256  TLSv1.3 Kx=any      Au=any  Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AESGCM(256) Mac=AEAD
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH       Au=RSA  Enc=AESGCM(256) Mac=AEAD
ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH     Au=RSA  Enc=CHACHA20/POLY1305(256) Mac=AEAD
DHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=DH       Au=RSA  Enc=CHACHA20/POLY1305(256) Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AESGCM(128) Mac=AEAD
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH       Au=RSA  Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES(256)  Mac=SHA384
ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(256)  Mac=SHA384
DHE-RSA-AES256-SHA256   TLSv1.2 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA256
ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES(128)  Mac=SHA256
ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(128)  Mac=SHA256
DHE-RSA-AES128-SHA256   TLSv1.2 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA256
ECDHE-ECDSA-AES256-SHA  TLSv1 Kx=ECDH     Au=ECDSA Enc=AES(256)  Mac=SHA1
ECDHE-RSA-AES256-SHA    TLSv1 Kx=ECDH     Au=RSA  Enc=AES(256)  Mac=SHA1
DHE-RSA-AES256-SHA      SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
ECDHE-ECDSA-AES128-SHA  TLSv1 Kx=ECDH     Au=ECDSA Enc=AES(128)  Mac=SHA1
ECDHE-RSA-AES128-SHA    TLSv1 Kx=ECDH     Au=RSA  Enc=AES(128)  Mac=SHA1
DHE-RSA-AES128-SHA      SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
AES256-GCM-SHA384       TLSv1.2 Kx=RSA      Au=RSA  Enc=AESGCM(256) Mac=AEAD
AES128-GCM-SHA256       TLSv1.2 Kx=RSA      Au=RSA  Enc=AESGCM(128) Mac=AEAD
AES256-SHA256           TLSv1.2 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA256
AES128-SHA256           TLSv1.2 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA256
AES256-SHA              SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
AES128-SHA              SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
```

   b. **Table with three default ciphersuites + 1 of your choice** (20 points)

Questions to Answer	First Cipher	Second Cipher	Third Cipher	Choice of Cipher
Name of cipher suite	TLS_AES_256_GCM_SHA384	TLS_CHACHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305
A. What they can encrypt (types/version of traffic, types of files, etc.)	Any data convertible to binary	Any data convertible to binary	Any data convertible to binary	Any data convertible to binary

B. What encryption algorithm does each use	AES256	ChaCha20/ Poly1305	AES128	ChaCha20/ Poly1305
C. Is the encryption algorithm a stream or block cipher	Block	Stream	Block	Stream
D. If it is a block cipher, what block cipher mode is used	GCM	N/A	GCM	N/A
E. What the key exchange protocol is used	Any	Any	Any	ECDH
F. What authentication is used	Any (plus GCM)	Any (plus Poly1305)	Any (plus GCM)	ECDSA (plus Poly1305)
G. What hash function is used	SHA 384	SHA 256	SHA 256	SHA 256
H. How many bits in the hash	384 bits	256 bits	256 bits	256 bits

2) Part 2:
   a. **Decrypt cipher and record the title, author, plaintext** (10 points)

      Dr. Suess: One fish, Two fish, Red fish, Blue fish

      One fish, Two fish, Red fish, Blue fish,
      Black fish, Blue fish, Old fish, New fish.
      This one has a little car.
      This one has a little star.
      Say! What a lot of fish there are.
      Yes. Some are red, and some are blue.
      Some are old and some are new.
      Some are sad, and some are glad,
      And some are very, very bad.
      Why are they sad and glad and bad?
      I do not know, go ask your dad.
      Some are thin, and some are fat.
      The fat one has a yellow hat.
      From there to here,
      From here to there,
      Funny things are everywhere.
      Here are some who like to run.

They run for fun in the hot, hot sun.

b. Encrypt the plaintext provided and upload to Canvas
(10 points)
Submitted File

3) Part 3:
   a. How many iterations for each cipher in 3 seconds using 8192 byte size blocks?
   (5 points)

   Cbc: 83146 iterations
   Gcm: 1196393 iterations

   b. How many megabytes can each cipher encrypt per second using 8192 byte size blocks?
   (5 points)

   Cbc: 228.5678
   Gcm: 3311.09846

   c. Which one is faster? Why?
   (5 points)

   GCM would be faster since it is performing more encryption iterations per second. As well, gcm is able to go over more blocks of data in the same amount of time. Hence, if both cbc and gcm were given the same plaintext, the gcm algorithm could encrypt it one or more times in less time.

4) Part 4:
   a. Submit the name of my favorite OS
   (10 points)
   Debian GNU/Linux

   b. Answer questions about my favorite OS
   (10 points)
   a. What mistake did I make?
      Uses ecb mode in AES
   b. What problem with this particular type of cipher block mode does this picture demonstrate?
      It will encrypt all data the same. So if 2 blocks are the exact same data it will be encrypt the same.
   c. How could I get rid of this problem?
      Use cbc or another mode in aes

   c. Submit an encrypted bmp of your favorite OS's mascot
   (15 points)

   Submitted file