Lab (optional) - NCL Fall 2017 Gymnasium

- This is an optional assignment, and is worth 10 points.
- The due date and time is Thursday, November 2 Midnight (right before the regular season game).
- Change the file name following the naming convention suggested below. Naming convention is as follows: homework, underscore, last name, first initial, and extension (e.g., Crypto-Assignment-ImG.docx).

- Log in to the following site: https://ncl.cyberskyline.com
- Go to Dashboard > NCL Fall 2017 Gymnasium > Select any <u>two</u> challenges except Wireless Access Exploitation.
- You will find a few questions for each challenge. Answer each question and provide necessary screenshots and explanation to justify your answer. Take advantage of the hints provided on the challenge.

Challenge 1: Network Traffic Analysis

1. What is the first username/password combination attempt to log into the server?
   User1/cyberskyline

   ```
   52 Request: USER user1
   73 Response: 331 Password required for user1
   59 Request: PASS cyberskyline
   ```

2. What software is the FTP server running? (Include name and version)

   ```
   220-FileZilla Server 0.9.53 beta
   ```

3. What is the first successful username/password combination?
   User1/metropolis

   ```
   Request: USER user1
   Response: 331 Password required for user1
   Request: PASS metropolis
   Response: 230 Logged on
   ```

4. What is the first command the user executes after logging on?

   ```
   46 Request: LIST
   ```

5. What file is deleted from the FTP server?
   Bank.cap

   ```
   55 Request: DELE bank.cap
   71 Response: 250 File deleted successfully
   ```

6. What file is uploaded to the server?
   Compcodes.zip

   ```
   60 Request: STOR compcodes.zip
   112 Response: 150 Opening data channel for file upload to server of "/compcodes.zip"
   ```

What is the MD5 sum of the uploaded file?
7. 3303628E25D43BE4E11CC8878C5C5878
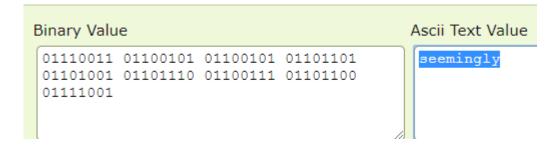8. What file does the anonymous user download?
   Compcodes.zip

```
16 Response: 150 Opening data channel for file download from server of "/compcodes.zip"
00 FTP Data: 1460 bytes
00 FTP Data: 1460 bytes
00 FTP Data: 1460 bytes
```

Change 2: Encryption

1. What is the plaintext password encoded in 0x636869636b656e?
   Chicken, 63=c 68=h 69=I 63=c 6b= k 65=e 6e=n , The password is in hexadecimal.

2. What is the plaintext password encoded by c2NyaWJibGU= ?

   scribble

   c2NyaWWJibGU=

3. What is the plaintext password encoded by

   01110011 01100101 01100101 01101101 01101001 01101110 01100111 01101100 01111001?

   Binary Value

   ```
   01110011 01100101 01100101 01101101
   01101001 01101110 01100111 01101100
   01111001
   ```

   Ascii Text Value

   seemingly

4. What is the plaintext encoded by

01011010 01101110 01001010 01110110 01100101 01010111 00111000 00111101?

Binary Value	Ascii Text Value
01011010 01101110 01001010 01110110 01100101 01010111 00111000 00111101	ZnJveW8=

ZnJveW8=

froyo