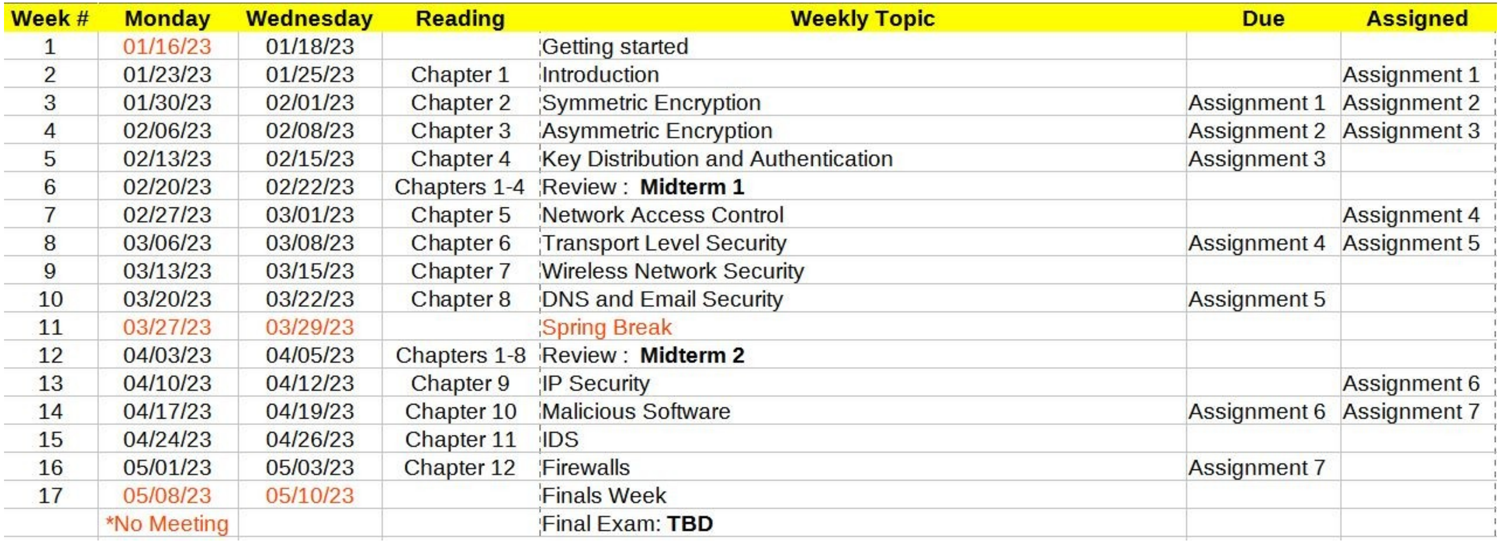
CS471
Security & Info Assurance

Welcome!
2/01/2023

CS471
Security & Info Assurance

Course Schedule



Week #	Monday	Wednesday	Reading	Weekly Topic	Due	Assigned
1	01/16/23	01/18/23		Getting started		
2	01/23/23	01/25/23	Chapter 1	Introduction		Assignment 1
3	01/30/23	02/01/23	Chapter 2	Symmetric Encryption	Assignment 1	Assignment 2
4	02/06/23	02/08/23	Chapter 3	Asymmetric Encryption	Assignment 2	Assignment 3
5	02/13/23	02/15/23	Chapter 4	Key Distribution and Authentication	Assignment 3	
6	02/20/23	02/22/23	Chapters 1-4	Review : **Midterm 1**		
7	02/27/23	03/01/23	Chapter 5	Network Access Control		Assignment 4
8	03/06/23	03/08/23	Chapter 6	Transport Level Security	Assignment 4	Assignment 5
9	03/13/23	03/15/23	Chapter 7	Wireless Network Security		
10	03/20/23	03/22/23	Chapter 8	DNS and Email Security	Assignment 5	
11	03/27/23	03/29/23		Spring Break		
12	04/03/23	04/05/23	Chapters 1-8	Review : **Midterm 2**		
13	04/10/23	04/12/23	Chapter 9	IP Security		Assignment 6
14	04/17/23	04/19/23	Chapter 10	Malicious Software	Assignment 6	Assignment 7
15	04/24/23	04/26/23	Chapter 11	IDS		
16	05/01/23	05/03/23	Chapter 12	Firewalls	Assignment 7	
17	05/08/23	05/10/23		Finals Week		
	*No Meeting			Final Exam: **TBD**		

CS471
Security & Info Assurance

Today

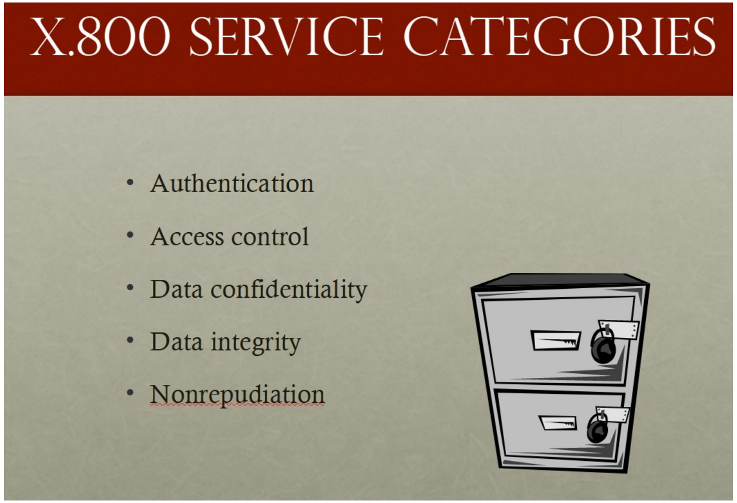
– Assignment 2

CS471
Security & Info Assurance

The X.800 service categories will be important for the entire semester.

As we examine security, this will be our measure.

- **X.800 Service Categories**
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Non-repudiation



X.800 SERVICE CATEGORIES

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation

CS471
Security & Info Assurance

Confidentiality

– What is ‘data confidentiality’?
– How can we provide confidentiality?
– What are the challenges?

CS471
Security & Info Assurance

Assignment 2:

Work with symmetric and asymmetric encryption using Kali Linux, gpg, md5sum, and steghide.

Demonstration

CS471
Security & Info Assurance

Notes:

```
# Create a file
echo "My name is Chris.
This is my secret message.. " >> plaintext.txt

# Change Permissions on this file
chmod 600 plaintext.txt

# Symmetric encryption with binary output
gpg --symmetric plaintext.txt
mv plaintext.txt.gpg ciphertext.txt.gpg
cat ciphertext.txt.gpg

# Symmetric encryption with ascii output
gpg --symmetric -a plaintext.txt
mv plaintext.txt.asc ciphertext.txt.asc
cat ciphertext.txt.asc

# Setup some prearranged listener
nc -l -p 31337 -q 1 > ciphertxt.txt.asc < /dev/null
# When the file is received, view it
cat ciphertxt.txt.asc

#our ascii armored, encrypted file to some prearranged listener
cat ciphertext.txt.asc | netcat 192.168.86.220 31337

# Decrypt the asymmetric message
gpg --decrypt ciphertxt.txt.asc

# Import asymmetric public key
gpg --import csmith.pub.key

# List the imported keys in local keyring
gpg --list-keys

# Create a public/private key pair
gpg --gen-key

gpg --list-keys
```

CS471
Security & Info Assurance

Notes:

```
# Export the public key in ascii format (Share this key)
gpg --export -a > public.key

# Sign the plaintext file with your private key
gpg -a --output plaintext.txt.asc.sig --sign plaintext.txt

# Encrypt the signed file to the recipient's key
gpg -e -a -u "You" -r "Christopher" plaintext.txt.asc.sig

# install stego tools
sudo apt-get install steghide
man steghide
steghide

# Download an image file (get your own file!!)
wget https://i.imgur.com/FkLjv4i.jpeg && cp FkLjv4i.jpeg image.jpg

# Embed a plaintext message in an image file
steghide embed -cf image.jpg -ef plaintext.txt -sf steg_image.jpg

# Check integrity
md5sum image.jpg
md5sum FkLjv4i.jpeg
md5sum steg_image.jpg

# Extract your secrets
steghide extract -sf steg_image.jpg

# Garbage
sudo adduser tmpuser
sudo adduser tmpuser sudo
su tmpuser
sudo deluser tmpuser

# root prompt using sudo
# aka interactive
sudo -i
```

CS471
Security & Info Assurance

Before next time:

- Read Chapter 3 from the textbook.
- Start Assignment 2

Next Time:
Chapter 3: Asymmetric Encryption

CS471
Security & Info Assurance

Thank you!