8/31 Scribe Notes

- Cryptography
  - Main goal is to protect assets from unintended view
  - Cryptographic Algorithms are an important element in security services
  - Evolved over time to include a wide variety of topics relating to the mathematics of alteration.
  - Techniques relying on difficult problems
  - Types:
    - Symmetric
    - Easily broken by knowing the algorithm/brute force attack
    - Asymmetric
    - Cert/Key
    - Hash
- Cryptanalysis
  - The study of how to break cryptographic security/data
  - Doesn’t need to be malicious/can be benevolent (black hat/white hat)
  - The keys are what need to be secured, not the algorithm
- Terms
  - Cryptosystem: A system for encryption & decryption
  - Encryption: Concealing a message
  - Decryption: The inverse to encryption
  - Plaintext: Raw data (What goes into the crypto algorithm); information in its original form
  - Ciphertext: Text that’s been converted
  - Cipher: Algorithm that will encrypt the data
    - Ciphers should be public to improve security
  - Key: Used to decrypt; Critical information used by cypher
- Kerckhoff’s Principle
  - The cipher method must not be secret and it must be able to fall into the hands of the enemy without inconvenience
- Symmetric Encryption
  - Attacks rely on the nature of the the algorithm, plus additional knowledge of plaintext characters and/or plaintext-ciphertext pairs
  - Can exploit characteristics of algorithm to break
- DES and Triple DES (Data Encryption Standard)
  - DES: Old standard, uses 64 bit plaintext blocks, with a 56 bit key to generate 64 bit ciphertext blocks
  - Problem: small key size means restrictive keys that are vulnerable to brute force
  - Triple DES is DES, but repeated three times, using two or three different keys
- AES (Advanced Encryption Standard)
  - Replaced DES, uses 128/192/256 bit keys
Questions:
How do we know the secure key channel is secure?
  ● Nothing can be fully and completely secure, however secure channels will be noted as such by trusted parties.

Say an encrypted message was intercepted. It would be a breach of integrity if whoever did the intercepting messed with the encryption and sent it onward (whether successfully decrypting or not), right? If so, how does cryptography ensure integrity of such a message?
  ● Cryptography will protect the message from being read, however if the attacker has means to directly tamper with the message, then the integrity of the message cannot be validated. However, it’s likely that unless the attacker is able to decode the message, whatever tampering is done will make the original message unreadable.

Given that larger keys are harder to break, is there any advantage of having a smaller key?
  ● Calculation speed

What’s an example of a secure key channel? is it possible for any channel on the internet to be 100% secure?
  ● HTTPS. SSL. No system is 100% secure.

If the same input is given multiple times to CBC, does the number of times it is feedback change each time it is encountered?
  ● No, the input is fed back once.

Why does key size limit block size?
  ● Symmetric key algorithms are designed to have key sizes equal to block sizes.

Should we assume that encrypted message is of same size?
  ● No because of padding

How does Encrypt block in block cipher decrypt padding part? Does padding part should always go through to encrypt block?
  ● Although the diagram shown made it look like padding isn’t retained through encryption/decryption, the padding is kept. It is treated the same as the other, informationally useful blocks of data.