Lecture 11

Summary – Chapter 2

- Symmetric block cipher
  - DES, 3DES
  - AES
- Random number
  - true random number
  - pseudorandom number
- Stream cipher
- The security of symmetric encryption depends on the secrecy of the key

Homework 1 - individual

- For Chapter 1 & 2
- Deadline: Oct. 2 (Monday), 11:59 pm
- We will use the blackboard submission time as your final timestamp
- 10% penalty per day for late submission

Network Security

Chapter 3

Public-Key Cryptography and Message Authentication

Public-Key Cryptography

Conventional cryptography

- traditional **private/secret/single-key** cryptography uses **one** key
- shared by both sender and receiver
- if this key is disclosed communications are compromised
- also is **symmetric**, parties are equal

Pros and cons

- Pros:
  - Encryption is fast for large amounts of data
  - Provide the same level of security with a shorter encryption key
  - By now, it’s unbreakable to quantum computing
- Cons
  - Key distribution assumes a secure channel
  - Does not protect sender from receiver forging a message & claiming it’s sent by sender
  - It does not scale well for large networks. It requires a separate key for each pair of communicating parties, which can result in a large number of keys to manage and protect.

Public-Key Cryptography

- In public-key schemes, each person has two keys
    - **Public key**: Known to everybody
    - **Private key**: Only known by that person
    - Keys come in pairs: every public key corresponds to one private key
- Uses number theory
    - Examples: Modular arithmetic, factoring, discrete logarithm problem, Elliptic logs over Elliptic Curves
    - Contrast with symmetric-key cryptography (uses XORs and bit-shifts)
- Messages are numbers
    - Contrast with symmetric-key cryptography (messages are bit strings)