时间：3月20，4：25-5：50

地点：SL212（science Lab）

458座位：2.4.6 rows

558座位：1.3.5.8 rows

1. Explain program
2. Example slides, examples in blackboard, assignment2
3. Figures

What is Confidentiality, Integrity, and Availability.

Passive Attacks ( given an attack, we should know what kind of attack it is)

Active Attack what kind do we got, and know the content.

Protocol layers

TCP/IP (UDP)

Different between link and network

Syscall used by cli and ser ( in C programming), don’t need to remember the parameters just name and its function.

Htows: convert host representation of it network rep.

Difference between Unconditional security and computational security

Caesar cipher

Mono cipher security (Frequency analysis can decrypt this cipher)

Playfair key matrix( encryption and decryption)

Row transposition cipher

Initial permutation ( 给你input 和table 要有output, 给你output 和 table 要有input)

S-Box( 同理)

Double DES

ECB, CFB, OFB, CTR : Advantage of different model and their limitation and their own figure

Key Distribution Scenario 的figure

Gcd

理解format， 需要的话老师会给出

Euler Totient Function牢记

不需要记住RSA 算法，只需要理解，老师考试的时候会给你内容

**DES必有！！！！**

**Public Key Encry**

**Number ？？？**