CH-06

1. Public-key announcement
2. Public-key authority (understand the pic and every step).
3. Public-key certificates (understand the pic and every step).
4. Simple secret key distribution (understand the step, and why it is not secure, and how to attack).
5. Diffie-hellman key exchange:
   1. what is primitive root, how to prove.
   2. Understand Diffie-hellman key exchange algorithm , how to prove that.
6. Man in the middle Attack

CH-07

1. Diff between Massage encryption, message authentication code(MAC)

Encryption needs reversible, MAC doesn’t need.

Encryption is one-to-one coding, MAC is many-to-one.

1. Diff between MAC and Hash

Hash doesn’t use key, MAC uses a symmetric key.

1. Understand the MAC (every part)
2. Understand Hash function (every part) (such as: “Why this requirement is important”)
3. Understand Simple Hash Functions
4. Know SHA-512 work

CH-08

1. Understand sample of HTTP
2. Base idea of SSL
3. How HTTP website work.

CH-09

1. What is Malicius Programs and its subclass definition
2. Difference between Worms and Virus
3. What is Compression Virus
4. Type of Virus and how to classify them and 特点 of each one
5. What is Trojan Horse
6. Difference between Email Virus and Worms
7. What is Rootkit, how to use rootkit to hack, and how rootkit works.

CH-10

1. What is Replay Attack, how it works and how to prevent, understand Protocol
2. What is Suppress-Replay Attack and how to prevent, understand protocol

CH-11

1. What is Phishing Email, how to prevent and tell.
2. Understand every step of PGP
3. What if a user has Multiple public pair, how to solve.
4. Understand PGP Message Format.

CH-12

1. What is Buffer Overflow Attack, why output is weird, what type of error it is( 2 type or more)
2. Understand every example.
3. How to counter buffer overflow attack ( at least two methods)

CH – 13

1. Login pages
2. Basic idea of SET and why we need Dual signature

CH-14

1. Understand every thing.