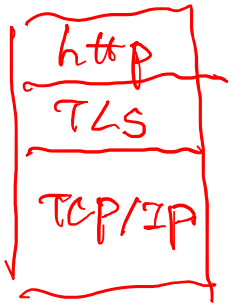
Design in security from the start

- When building a new system, include security as part of the design considerations rather than patching it after the fact
  - A lot of systems today were not designed with security from the start, resulting in patches that don't fully fix the problem!
- Keep these security principles in mind whenever you write code!

① http → https ⟶ TLS OSI

② IPSEC.



Story…

- The bear race
- **Takeaway:** Even if a defense is not perfect, it is important to always stay on top of best security measures

I don’t have to outrun the bear. I just have to outrun you

Human Factors

- The users
  - Users like convenience (ease of use)
  - If a security system is unusable, it will be unused
  - Users will find way to subvert security systems if it makes their lives easier
- The programmers
  - Programmers make mistakes
  - Programmers use tools that allow them to make mistakes (e.g. C and C++)
- Everyone else
  - Social engineering attacks exploit other people's trust and access for personal gain

Supplementary materials

- Internet Security Glossary, v2 – produced by Internet Society (ISOC) https://datatracker.ietf.org/doc/html/rfc4949
- X.800 – OSI network security

  https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-REC-X.800-199103-I!!PDF-E&type=items
- TTU Library webinars for fall 2025

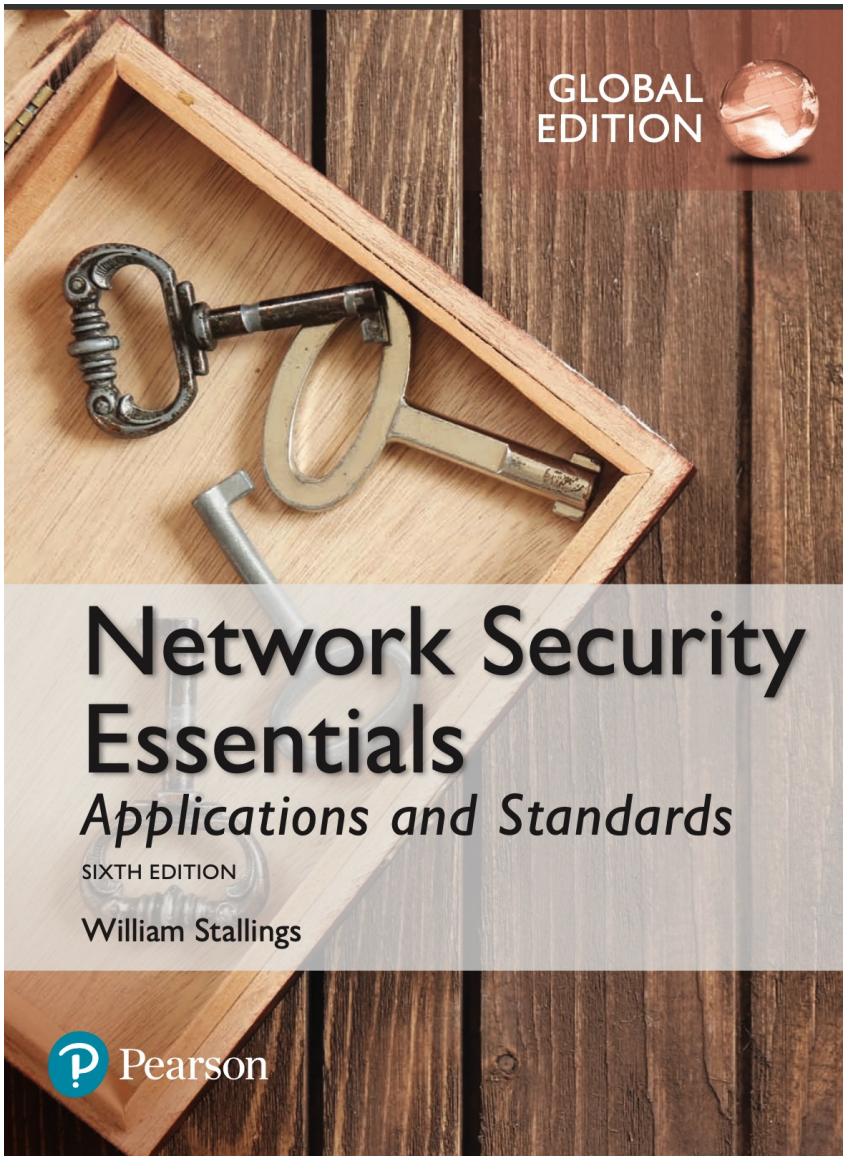
  https://cal.library.ttu.edu/calendar?cid=4506&t=d&d=0000-00-00&cal=4506&ct=75348&inc=0

Summary for Chapter 1

- Have learned:
  - Security requirements
  - Attack models
  - X.800 secure architecture, security services, mechanisms

Review Questions

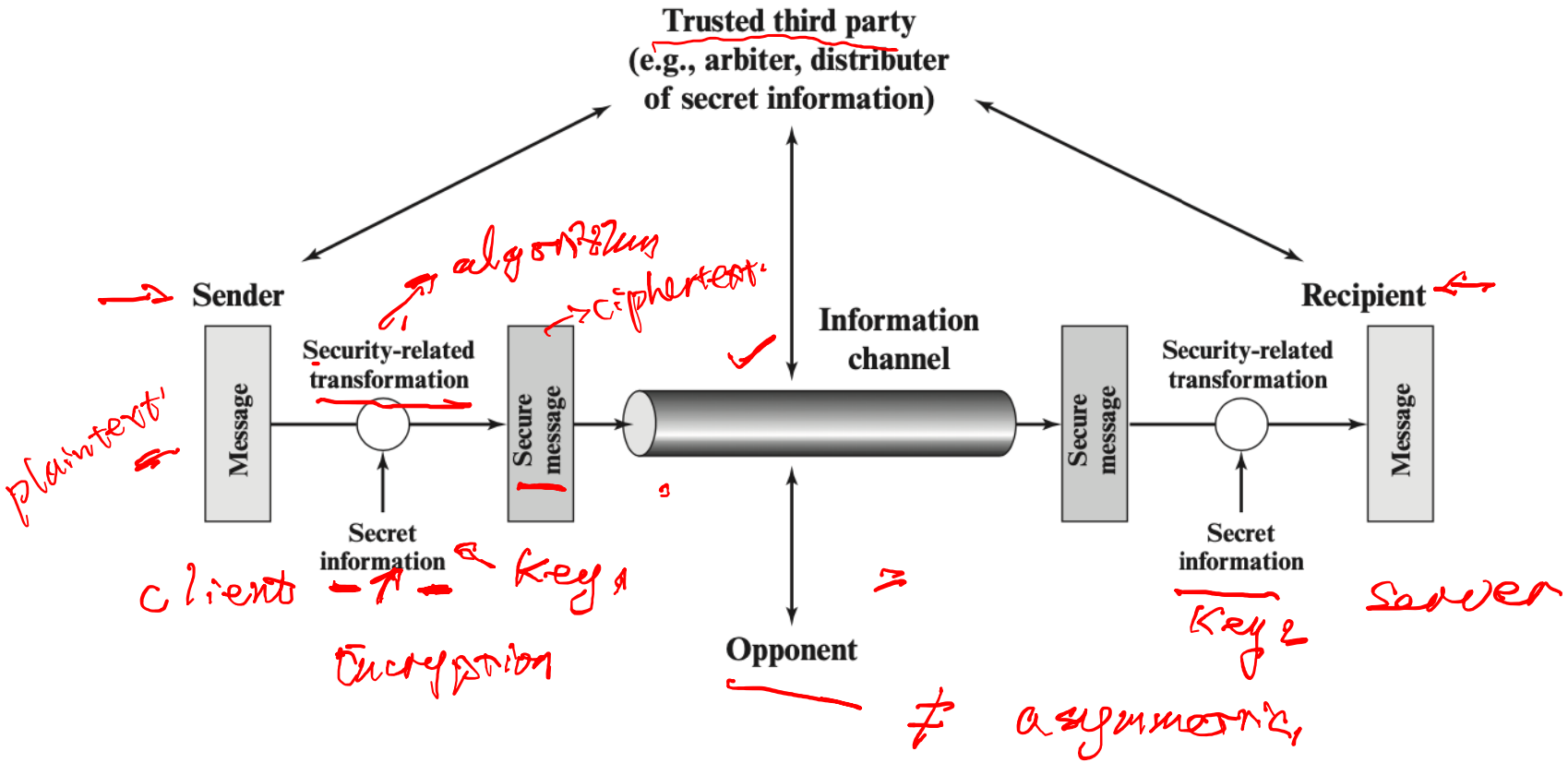
- William Stallings (WS), "Network Security Essentials", 6th Global Edition
- RQ 1.1 - 1.3
- Prob 1.5



Symmetric Encryption and Message Confidentiality

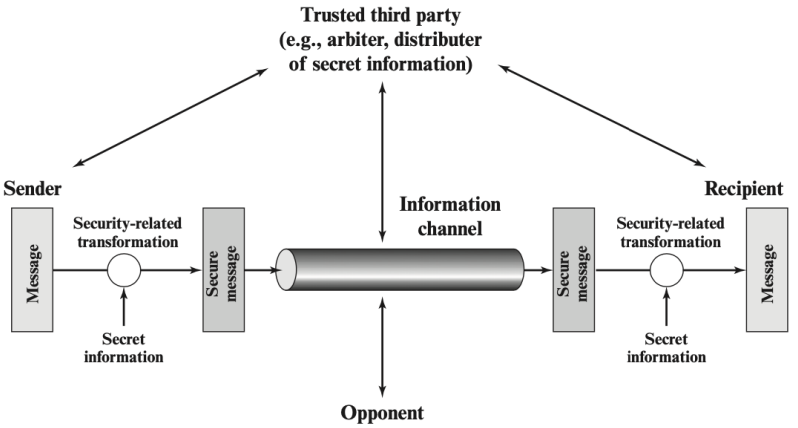
Chapter 2

Model for network security



Model for network security

- Using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

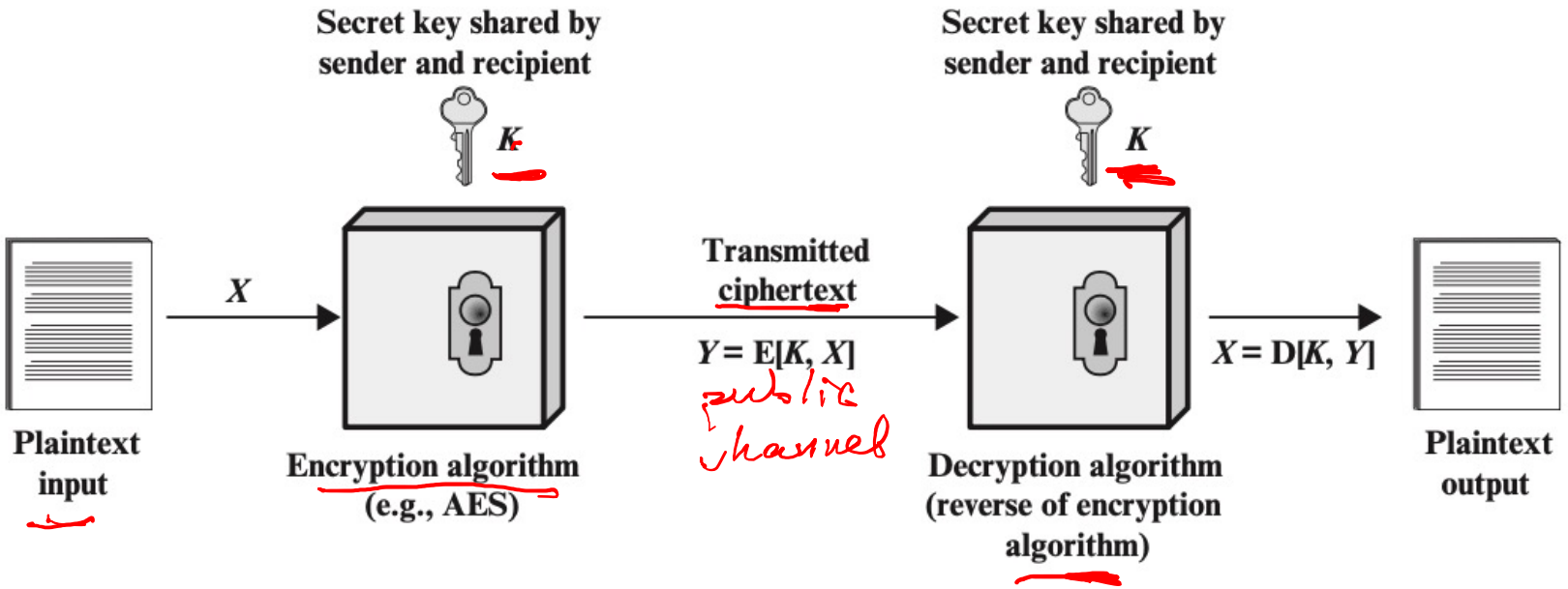


Symmetric Encryption Principles

Symmetric encryption

- Sender and recipient share a common/same key
- Was the only type of cryptography, prior to invention of public-key in 1970's

Simplified model of symmetric encryption



Symmetric encryption

- Has five ingredients
  - **Plaintext**: the original message or data
  - **Encryption algorithm**: performs various substitutions and transformations on the plaintext
  - **Secret key**
  - **Ciphertext**: the coded message
  - **Decryption algorithm**: takes the ciphertext and the same secret key and produces the original plaintext

Other basic terminology

- **cipher** - algorithm for transforming plaintext to ciphertext
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering plaintext from ciphertext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key

Requirements

- Two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver

  $Y = E_K(X)$

  $X = D_K(Y)$
- assume encryption algorithm is known
- the security of symmetric encryption depends on the secrecy of the key
- implies a secure channel to distribute key

TA & Grader

- TA Name: Zambare, Pallavi (Project, Review & Quiz)
- Email: pzambare@ttu.edu
- Reminder: Submit the names and emails of your group members to

FALL 2025 CS5342 PROJECT GROUP NAMES.xlsx

- Grader Name: Danso, Kwesi (Homework, Quiz, Exam grading)
- Email: kdanso@ttu.edu