Network Security

Internet Technologies
COMP90007

Reading

- Please read sections 8.1 to 8.5 from the book for this topic and skim the rest of the chapter related to the slides that we will cover for the rest of the topic.

What is Network Security?

- Network security is a combo of 4 related areas:
  - **Secrecy** (Keeping information hidden from a general audience)
  - **Authentication** (Ensuring the user you are giving content to has valid credentials)
  - **Integrity control** (Ensure that a content has not been tampered with)
  - **Non-repudiation** (Prove a content was created by a named user)

What is Network Security?

- All of the 4 above are **equally valid** and has been around for all systems for some time, but have different and sometimes *more challenging implications in a networked environment*

- Aspects of security can be found at all layers of a protocol stack, **there is no way to secure a network by building security into one layer only**

- Most security implementations are **based on common cryptographic principles** and appear on almost all layers, and we look into this area of study a bit first

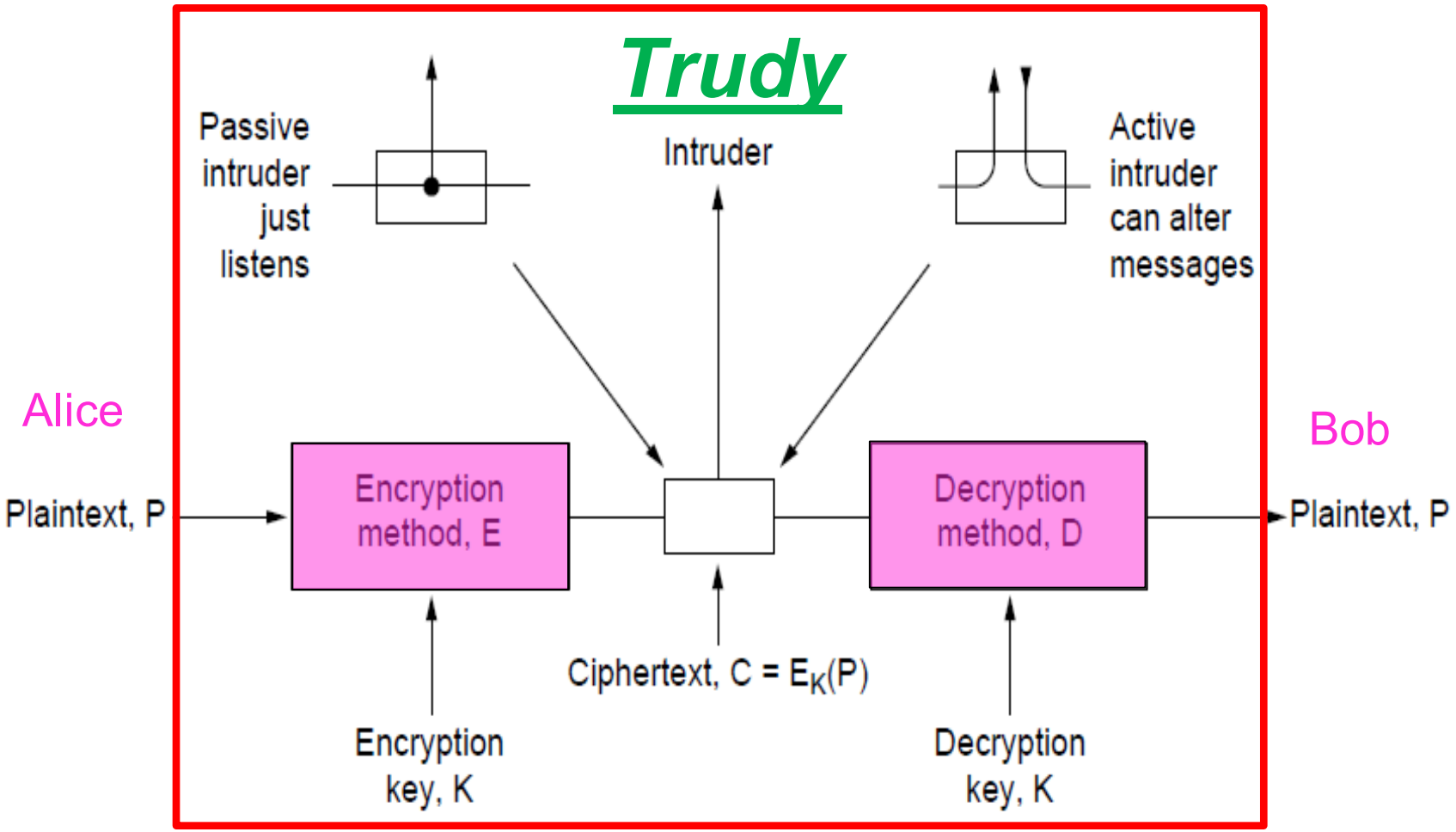
Cryptography

- A key area/set of algorithms for creating secrets, authenticating users, making sure messages are not tampered with, and edits are not denied by the original author.

A Simple Example

- Transform every character to the next one in the alphabet for a given plaintext (and “z” becomes “a” to circle around the end)
- Input plaintext
  - “where”
- Output ciphertext
  - “xifsf”
- Methods: **Decryption**/unlocking is the simple method to go back in the alphabet to reverse the effect of **encryption**/locking

Basic Encryption Model



By the Way: Is Intruder Always a Distant "Cool" Hacker?

Adversary	Goal
Student	To have fun snooping on people's email
Cracker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Businessman	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by email
Con man	To steal credit card numbers for sale
Spy	To learn an enemy's military or industrial secrets
Terrorist	To steal germ warfare secrets

Key Concepts

- Three foundations:
  - Plaintext
  - Keys (+function)
  - Ciphertext
- Plaintext messages to be encrypted can be transformed (encrypted/decrypted) by a function that is parameterized by a key, the output of the transformation process is ciphertext
- Kerckhoff's principle: Cryptographic algorithms and related functions (E, D) are public; only the keys (K) are secret

The Notation

- C = ciphertext, P = plaintext, E = encryption, D =decryption, K = key
- $C = E_K(P)$
- $P = D_K(C)$

- **$D_K(E_K(P)) = P$**
- In fact what we commonly want in many simple crypto-based network security scenarios is efficient methods where

$$D_{K1}(E_{K2}(P)) = P \textbf{ if and only if } K1=K2$$

Keys Play an Important Role: Why?

- A key is a **string that allows the selection** of one of many potential encryptions
- The **key can be changed** as often as required
- **Algorithms are more likely to be at the hands of attackers eventually**, as/but cannot be changed frequently
- Note that **Cipher is a term** commonly used as the term for algorithm here
- The size of the overall key space is determined by the number of bits in the key string
- The **longer the key, the more effort is required to break a given encryption**

A most common function used in ciphers: XOR

- An XOR is an “exclusive or” function used regularly
- A XOR B means A or B, but not both
- XOR is commonly used in cryptography
- Recall: We saw XOR in checksums etc before

A	B	A XOR B
F	F	F
F	T	T
T	F	T
T	T	F

Truth values	Binary Equivalents
T	1
F	0

Some Main Types of Ciphers

- *Substitution* cipher
  - Each letter of group of letters is replaced systematically by other letters or groups of letters
- *Transposition* cipher
  - All letters are re-ordered without disguising them
- *One-time pad*
  - Uses a random bit string as a key: then convert the plaintext into a bit string and XOR the two strings bit by bit
  - Hard to break
  - How to share the random key and its size are the issues

Another Example: Substitution cipher example

- Substitution ciphers replace group of letters in the message with another group of letters based on a key with an intension to disguise the message, 26 letter simple key given with the simple example below.

plaintext:	a b c d e f g h i j k l m n o p q r s t u v w x y z
ciphertext:	Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

- If “were” was the ciphertext received then it was originally

“bcdc”

…and will be when decrypted as well…

Modern Key-based Algorithms

Two main categories:

1) **Symmetric key algorithms** use the same key for both encryption and decryption

- Symmetric key algorithms can use transposition, substitution and a combination of both to encrypt and decrypt
- We discuss them first…