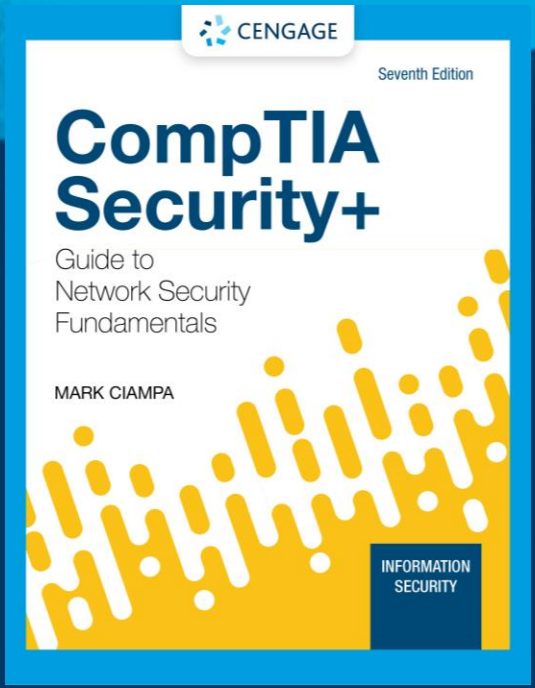
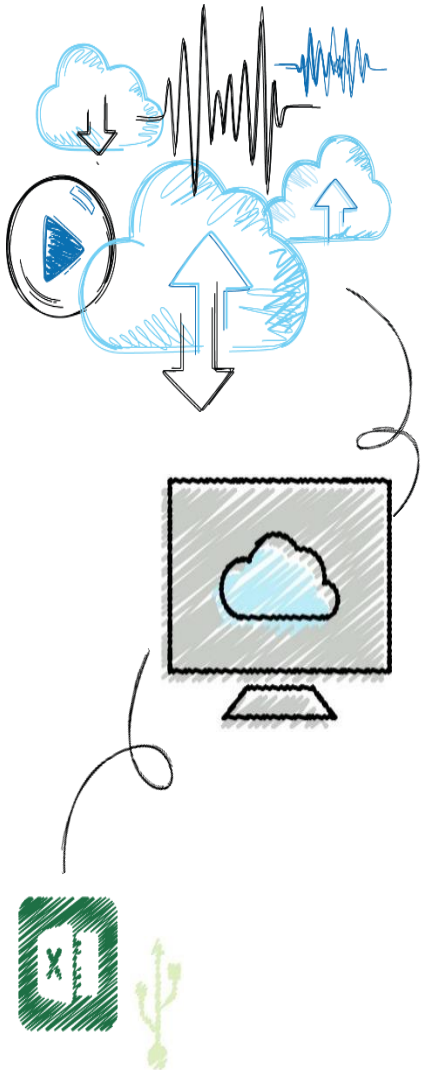


Principles of Cyber Security

Lecture 10: Traditional Ciphers_IV

CENGAGE



Objectives

10.1 Describe Substitution Ciphers algorithms (Caesar Cipher).

Caesar Cipher

- The Caesar Cipher is a monoalphabetic cipher in which **each letter is replaced** in the encryption by another letter a **fixed "distance"** away in the alphabet.

- **For example**, A is replaced by C, B by D, ..., Y by A, Z by B, etc. *What is the key?*
  - ***What is the size of the keyspace?***

Substitution Ciphers

❖ Caesar Cipher

- This is an example of Caesar Cipher in which each letter in the alphabet is **rotated by three letters** as shown.

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

↓

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Substitution Ciphers

❖Caesar Cipher

- Let us try to ***encrypt*** the message

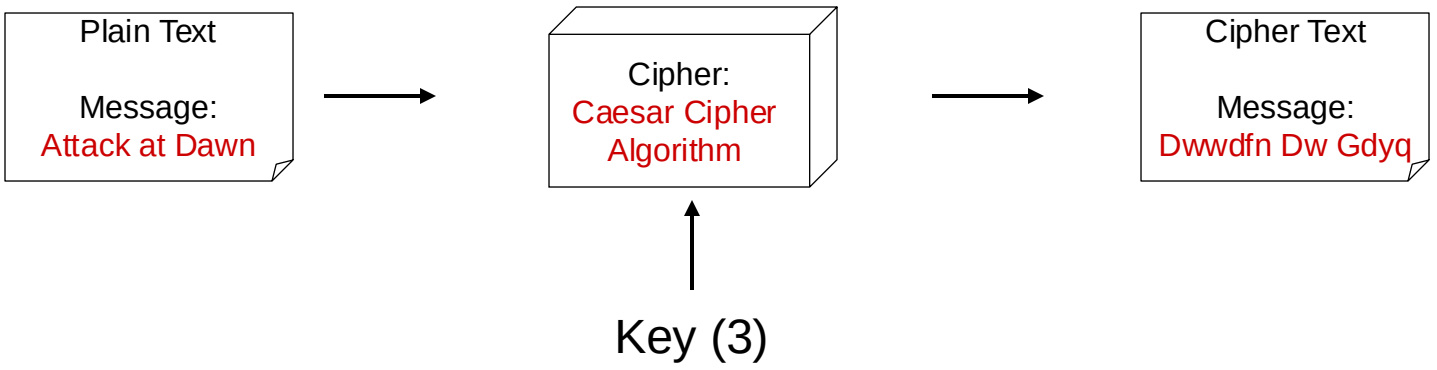
****Attack at Dawn**

➢ **Assignment:** Each student will exchange a secret message with his/her closest neighbor about some other person in the class and the neighbor will decipher it.

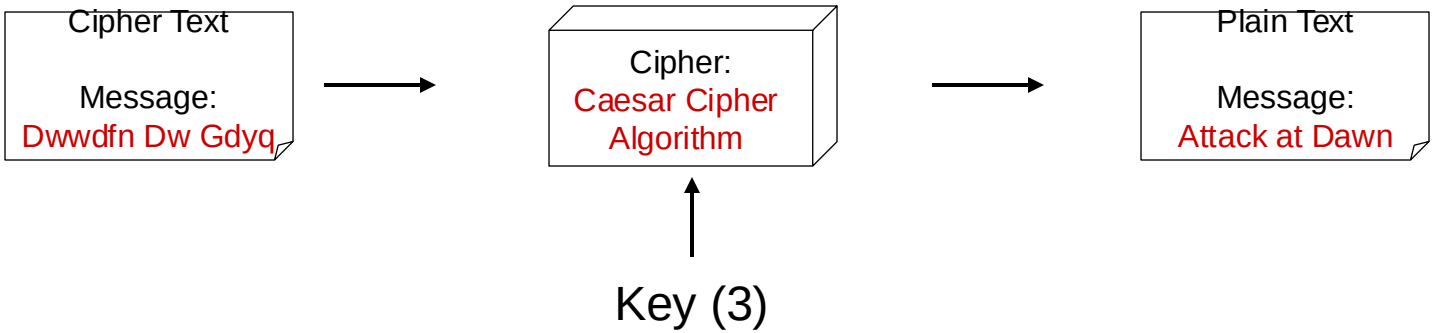
Substitution Ciphers

Caesar Cipher

Encryption



Decryption



How many different keys are possible?

Simple Substitution

- A simple substitution cipher is an injection (1-1 mapping) of the alphabet into itself or another alphabet. ***What is the key?***
- A simple substitution is breakable; we could try all k! mappings from the plaintext to ciphertext alphabets. ***That's usually not necessary.***
- Redundancies in the plaintext (letter frequencies, digrams, etc.) are reflected in the ciphertext.
  - ***Not all substitution ciphers are simple substitution ciphers.***

Thank you

CENGAGE