

# Cryptography and Information Theory

## **Cryptography Overview**

Sang-Yoon Chang, Ph.D.

## **Module Objectives:**

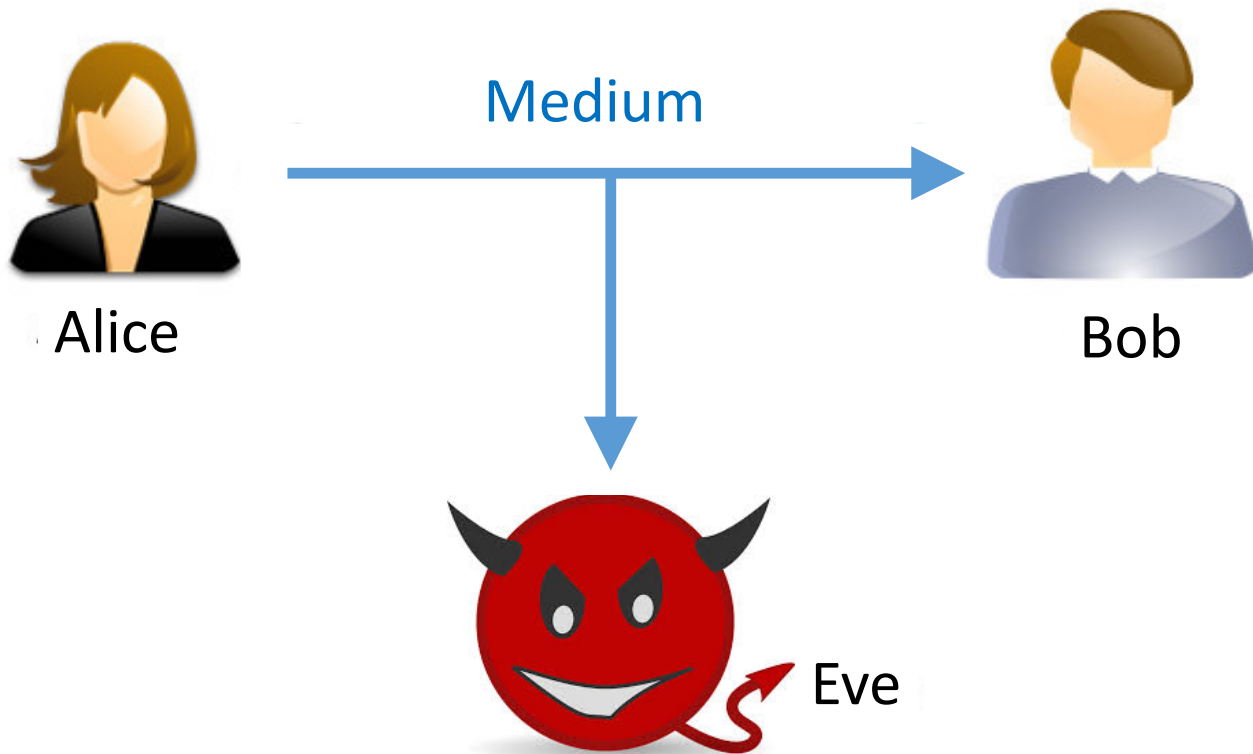
1. Alice, Bob, Eve, and Other Terminology
2. Kerckhoff's Principle
3. Security by Obscurity



## Alice, Bob, and Eve



# Alice, Bob, and Eve





## Cryptography Terminology

**Plaintext** (p) - the original message

**Ciphertext** (c) - the coded message

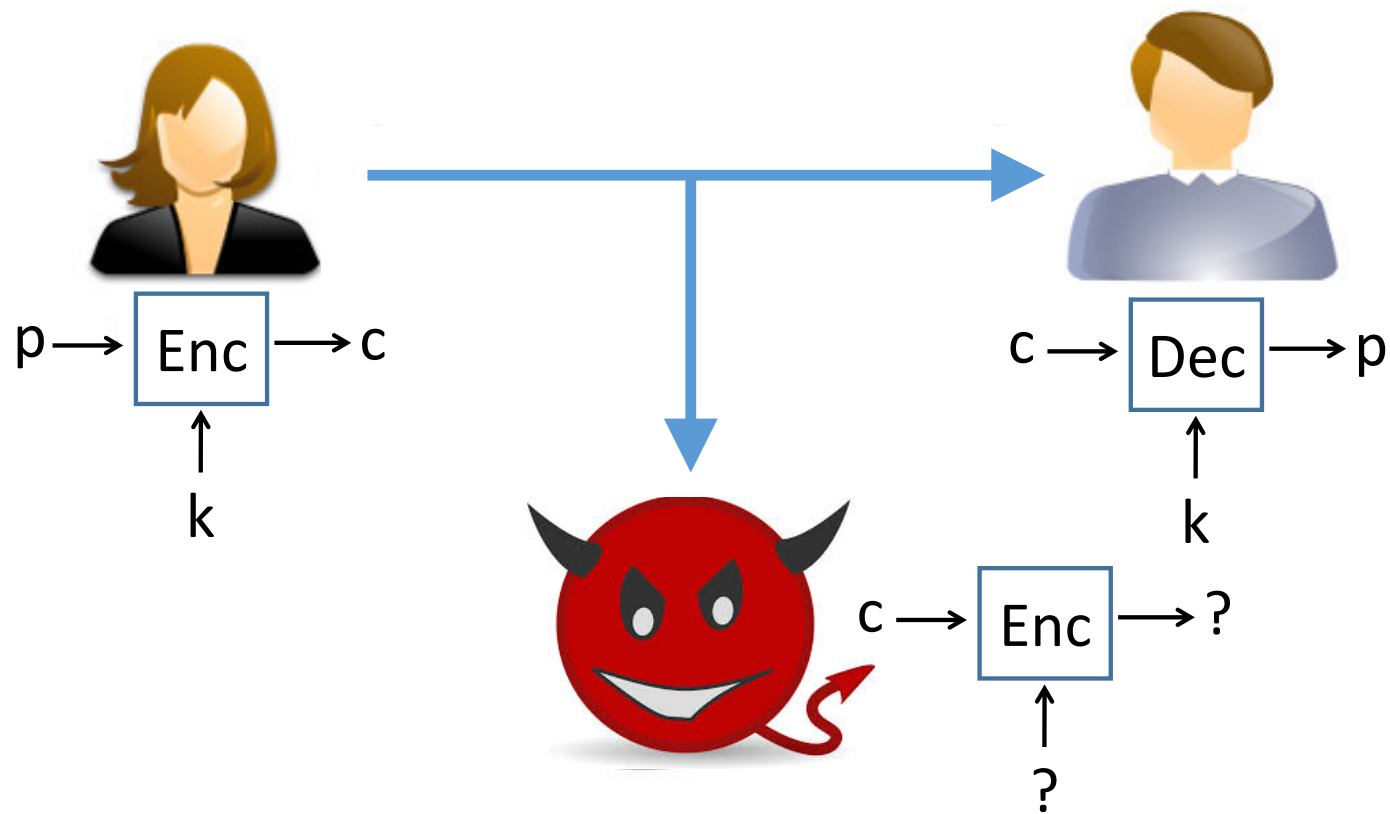
**Cipher** - the algorithm used for  
transforming p to c

**Key** (k) - the information only known  
to Alice and Bob

**Encrypt** -  $p \rightarrow c$

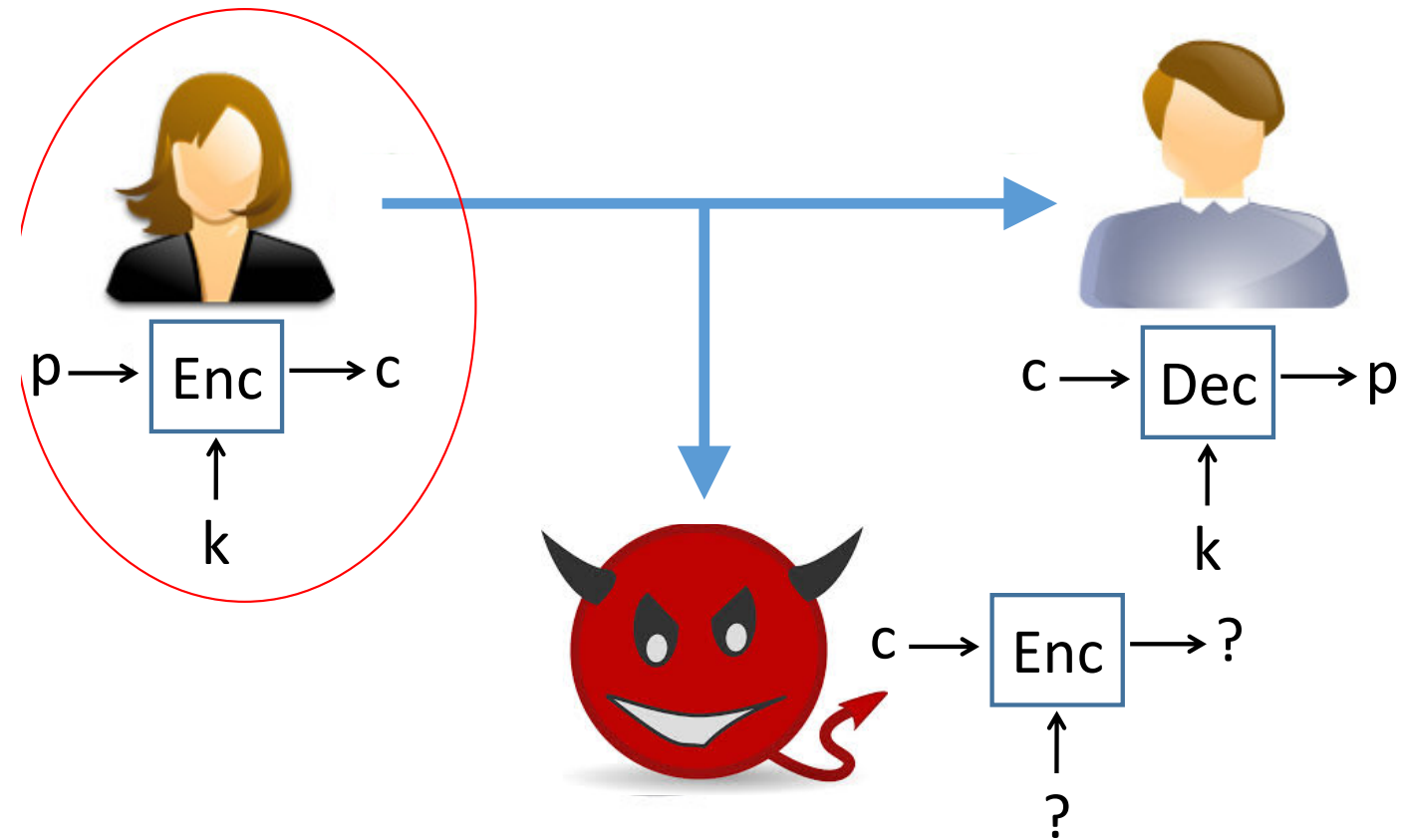
**Decrypt** -  $c \rightarrow p$

# Cryptography Terminology

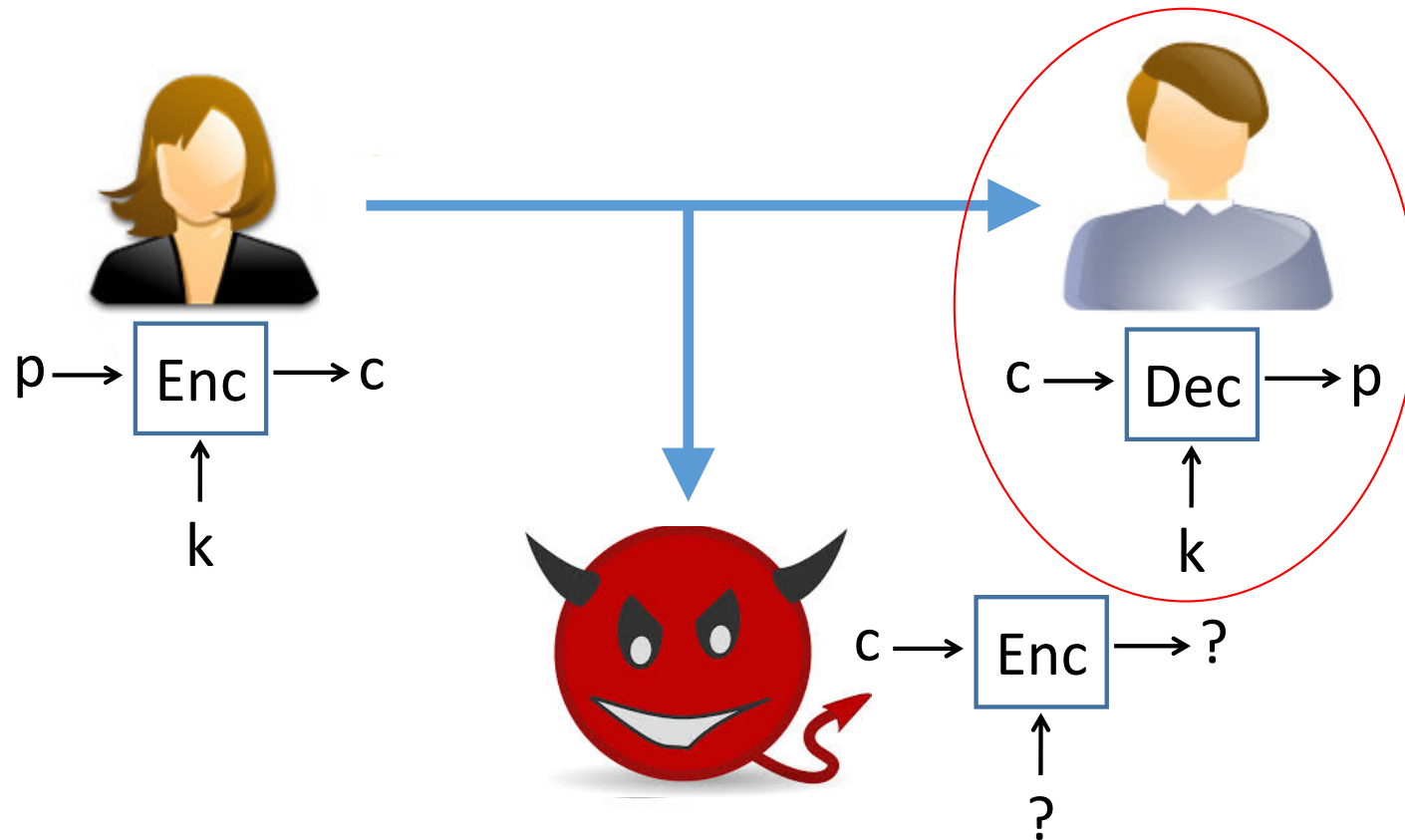




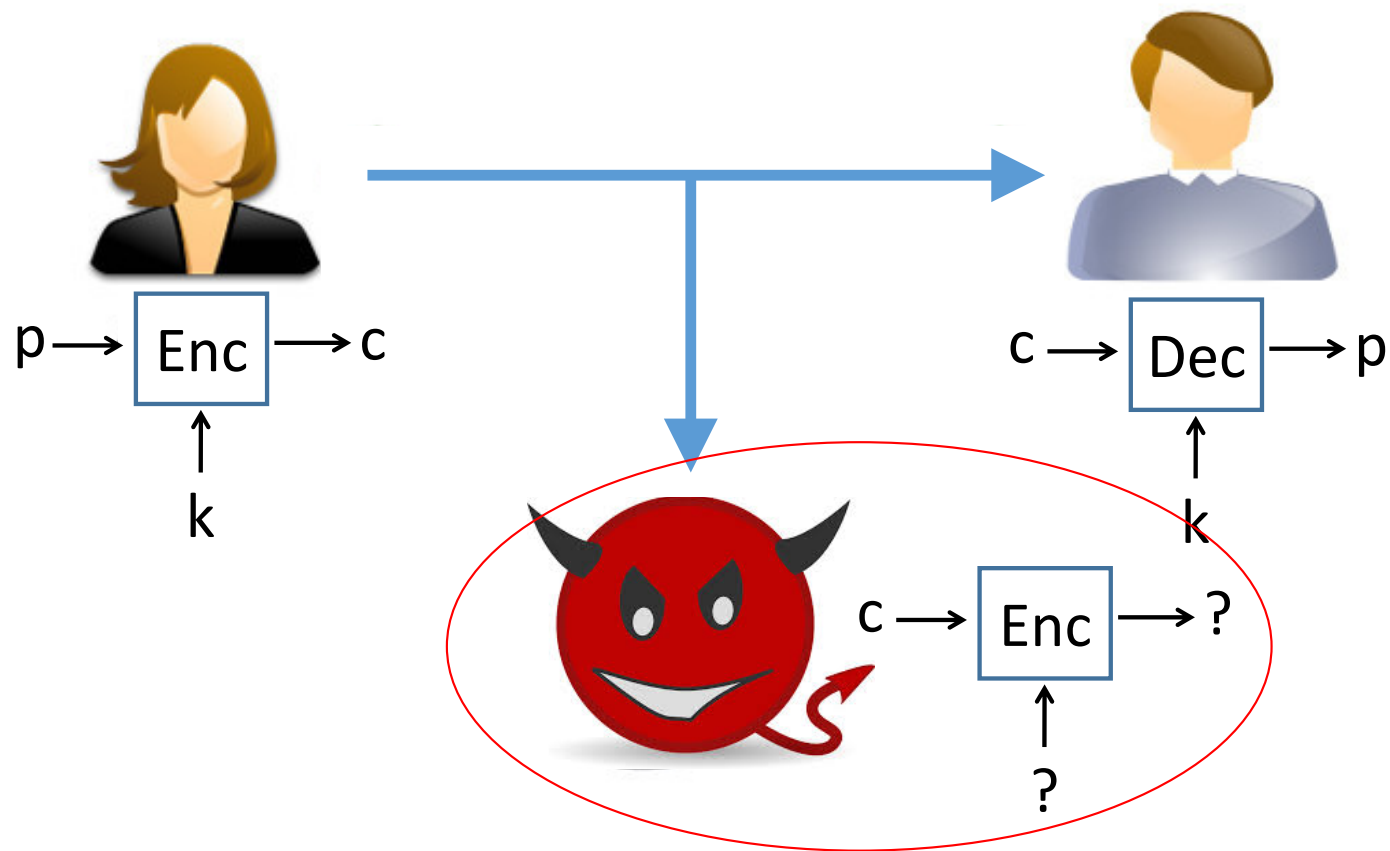
# Cryptography Terminology



# Cryptography Terminology



# Cryptography Terminology



# **Cryptography Terminology**

**Cryptography** - the study of encryption and decryption techniques

**Cryptanalysis** – codebreaking and deciphering ciphertext without the key

**Cryptology** – the field of cryptography and cryptology



## Threat Model



How much does the attacker know?

What does the attacker not know?



## **Kerckhoff's Principle**

- Also called Open Design or Shannon Maxim
- The attacker knows the system



## **Kerckhoff's Principle**

- Also called Open Design or Shannon Maxim
- The attacker knows the system
- Security relies on the secrecy of keys

## **Kerckhoff's Principle**

- Also called Open Design or Shannon Maxim
- The attacker knows the system
- Security relies on the secrecy of keys
- Common design principle among security experts



## **Security by Obscurity**

- The attacker does not know the system because the algorithms/protocols are proprietary and confidential
- History shows that the approach is vulnerable, e.g., reverse engineering

# Steganography

- Related to Security by Obscurity  
but focuses more on concealing the  
presence of the message
- Typically the security is breached once  
the concealment method is known

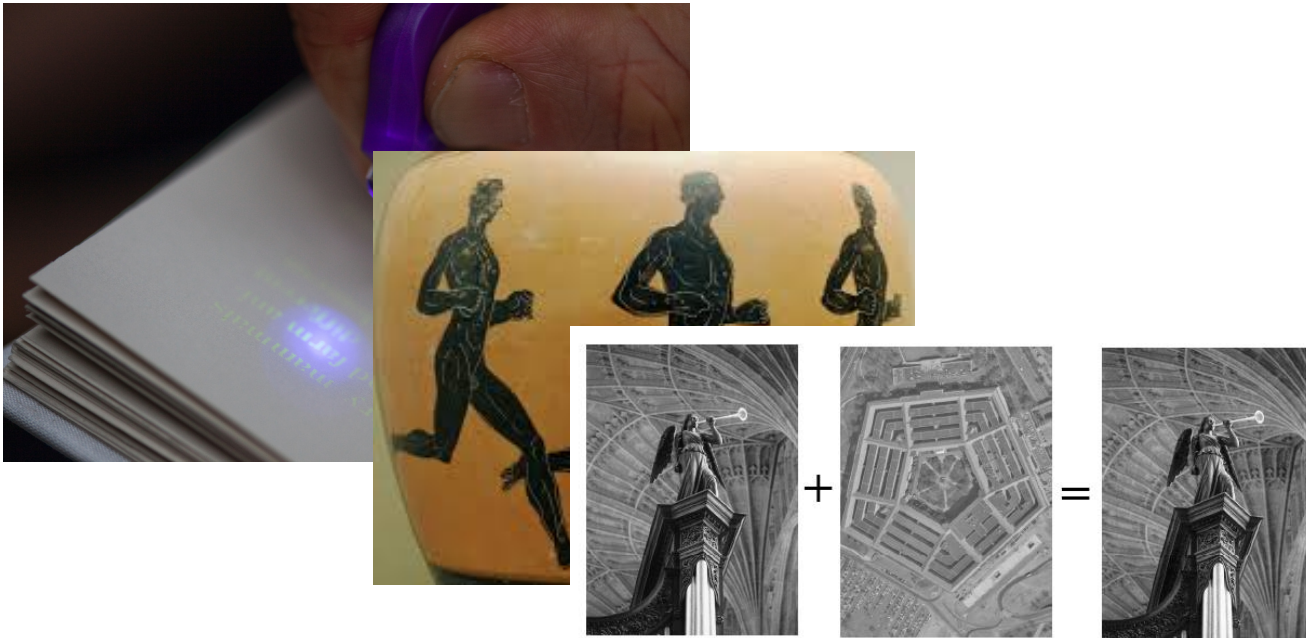
# Steganography



# Steganography



# Steganography





# Steganography



Since everyone can read, encoding text in neutral sentences is doubtfully effective

# Steganography



Since everyone can read, Encoding Text in Neutral sentences is doubtfully effective

# Steganography (A Puzzle for Inspector Morse)

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the summer examination package.

All entry forms and fees forms should be ready for final despatch to the Syndicate by Friday 20<sup>th</sup> or at the very latest, I'm told, by the 21<sup>st</sup>.

Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basis O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.



# Steganography (A Puzzle for Inspector Morse)

Dear George,

Greetings to all at Oxford. Many thanks for your  
letter and for the summer examination package.

All entry forms and fees forms should be ready  
for final despatch to the Syndicate by Friday  
20<sup>th</sup> or at the very latest, I'm told, by the 21<sup>st</sup>.

Admin has improved here, though there's room  
for improvement still; just give us all two or three  
more years and we'll really show you! Please  
don't let these wretched 16+ proposals destroy  
your basis O and A pattern. Certainly this  
sort of change, if implemented immediately,  
would bring chaos.

Sincerely yours.

## Kerckhoff's vs. Obscurity

- History shows that Security by Obscurity is vulnerable
- We assume Kerckhoff's Principle moving forward
- The scope of secrecy is clearly defined, and everything else can be known to the attacker

