# Shannon’s Theory of Secrecy System

Dept. of Computer Science & Engg.
IIT Kharagpur, India

Teacher: Dipanwita Roy Chowdhury

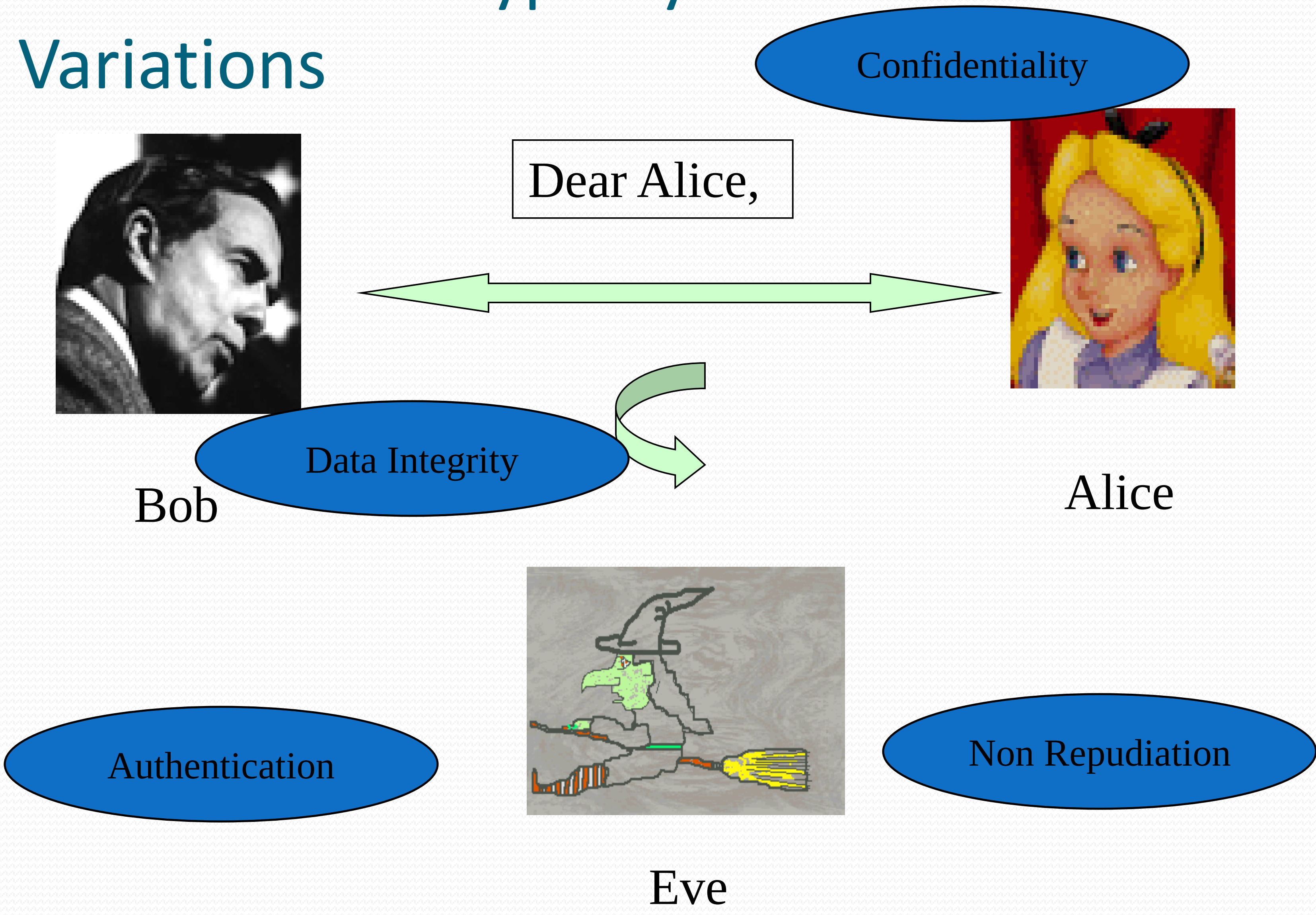
# Shannon’s Information Theory Paper

- “Mathematical Theory of Communication”, published in 1948
- Main claim:
  - All sources of data have a **rate**
  - All channels have a **capacity**
  - If the **capacity** is greater than the **rate**, transmission with **no errors** is possible
- Introduced concept of **entropy** of a random variable/process

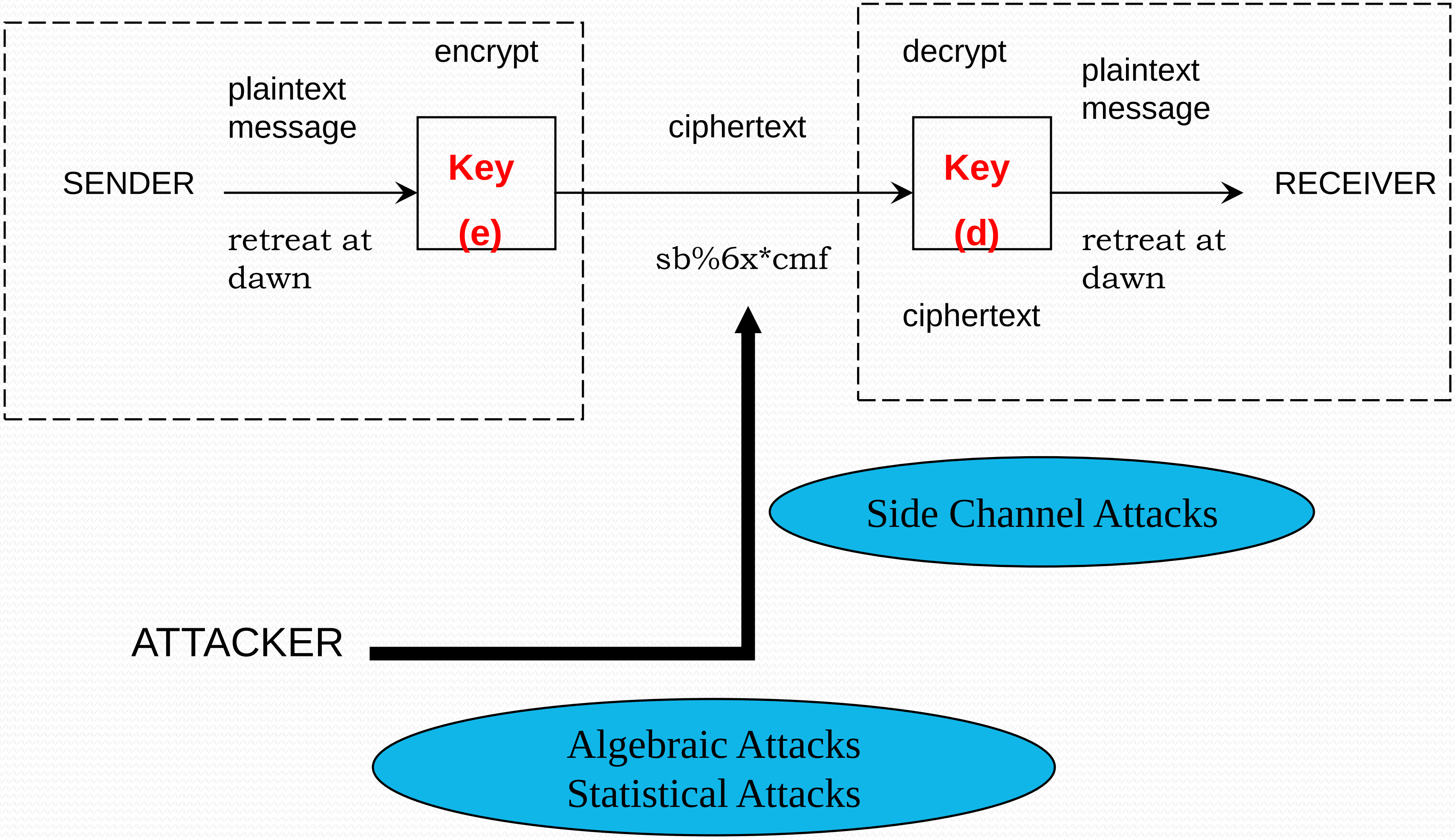
# Definition of a Cryptosystem:

- A cryptosystem can be viewed as a distribution of plaintexts P, a set of ciphertexts C, a distribution of possible keys (K) and an encoding transformation, with its inverse (D).

# Definition of Cryptosystem Modern Variations



# Cryptographic Algorithms



# Shannon’s 1948 Paper

- Published one year after his monumental “information theory” paper
- “transformed cryptography from art to science”

# Main Contributions

- Notions of **theoretical security** and **practical security**
- Observation that the secret is all in the key, not in the algorithm
- **Product ciphers** and **mixing transformations** – inspiration for **DES, AES and …………**
- Proof that **Vernam's cipher** (one-time pad) was **theoretically secure**

# Theoretical and Practical Security

# Theoretical and Practical Security

- **Theoretically secure** cryptosystems cannot be broken – even by an all-powerful adversary
- **Practically secure** cryptosystems "require a large amount of work to solve"
- Bad news:
  - The only **theoretically secure** cryptosystem is the **one-time pad**
  - The only **practically secure** cryptosystem is… the **one-time pad**

# Shannon's theory

- 1949, "Communication theory of Secrecy Systems" in Bell Systems Tech. Journal.
- Two issues:
  - What is the concept of perfect secrecy? Does there any cryptosystem provide perfect secrecy?
    - It is possible when a key is used for only one encryption
  - How to evaluate a cryptosystem when many plaintexts are encrypted using the same key?

# Shannon’s 1949 Paper

- Approaches to evaluate the security of Cryptosystem
  - Computational Security
  - Provable Security
  - Unconditional Security

# Computational Security

- Concerns the computational effort required to break a cryptosystem

  Definition

  A Cryptosystem is said to be computationally Secure if the best algorithm for breaking it requires atleast N operations where N is some specified, very large number.

  Problem - No known cryptosystem can be proved to be secure.

  - Specific attack like Exhaustive Key Search

# Provable Security

Definition

A Cryptosystem is said to be provably Secure if the security of the system can be reduced to some well-studied problem that is considered to be difficult

Example "A given cryptosystem is secure if a given integer n cannot be factored"

- relative not an absolute proof

# Unconditional Security

Definition

A cryptosystem is said to be unconditionally secure if it cannot be broken, even with infinite computational resources.

- it cannot be studied from the point of view of computational complexity as we allow computation time is infinite
- can be studied with Probability Theory

# One-Time Pad

- Unconditional security !!!
- Described by Gilbert Vernam in 1917
- Use a random key that was truly as long as the message, no repetitions

$$P = C = K = (Z_2)^n \quad x = (x_1, \ldots, x_n) \quad K = (K_1, \ldots, K_n)$$

$$e_K(x) = (x_1 + K_1, \ldots, x_n + K_n) \mod 2$$

For ciphertext $y = (y_1, \ldots, y_n)$

$$d_K(y) = (y_1 + K_1, \ldots, y_n + K_n) \mod 2$$

# Example: one-time pad

- Given ciphertext with Vigenère Cipher: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

Decrypt by hacker 1:

```
CT: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
Key: pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
PT:  mr mustard with the candlestick in the hall
```

Decrypt by hacker 2:

```
CT: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
Key:pftgpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt
PT:miss scarlet with the knife in the library
```

Which one?

# Problem with one-time pad

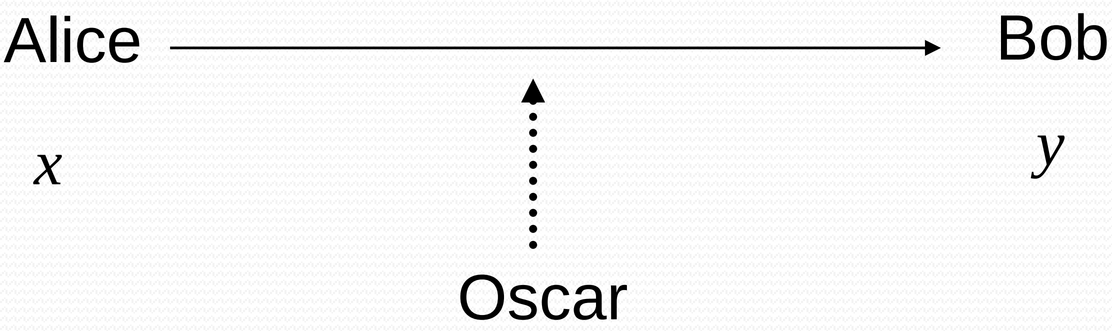
- Truly random key with arbitrary length?
- Distribution and protection of long keys
  - The key has the same length as the plaintext!
- One-time pad was thought to be unbreakable, but there was no mathematical proof until Shannon developed the concept of perfect secrecy 30 years later.

# Perfect secrecy

- When we discuss the security of a cryptosystem, we should specify the type of attack that is being considered
  - Ciphertext-only attack
- Unconditional security assumes infinite computational time
  - Theory of computational complexity ×
  - Probability theory ˅

# Perfect secrecy

- **Definition:** A cryptosystem has perfect secrecy if $\Pr[x|y] = \Pr[x]$ for all $x \in P$, $y \in C$
- Idea: Oscar can obtain no information about the plaintext by observing the ciphertext



# Elementary Probability Theory

# Discrete random variable

- **Def:** A *discrete random variable*, say **X**, consists of a finite set $X$ and a probability distribution defined on $X$.
- The probability that the random variable **X** takes on the value $x$ is denoted $\Pr[\mathbf{X}=x]$ or $\Pr[x]$
- $0 \le \Pr[x]$ for all $x \in X$, $\sum_{x \in X} \Pr[x] = 1$

# Discrete random variable

- Ex. Consider a coin toss to be a random variable defined on {head, tails} , the associated probabilities Pr[head]=Pr[tail]=1/2
- Ex. Throw a pair of dice. It is modeled by Z={(1,1), (1,2), …, (2,1), (2,2), …, (6,6)}

  where Pr[(i,j)]=1/36 for all i, j.

  sum=4 corresponds to {(1,3), (2,2), (3,1)} with probability 3/36

# Joint and conditional probability

- **X** and **Y** are random variables defined on finite sets $X$ and $Y$, respectively.
- **Def:** the joint probability $\Pr[x, y]$ is the probability that **X**$=x$ and **Y**$=y$
- **Def:** the conditional probability $\Pr[x|y]$ is the probability that **X**$=x$ given **Y**$=y$

$$\Pr[x, y] = \Pr[x|y]\Pr[y] = \Pr[y|x]\Pr[x]$$

# Bayes' theorem

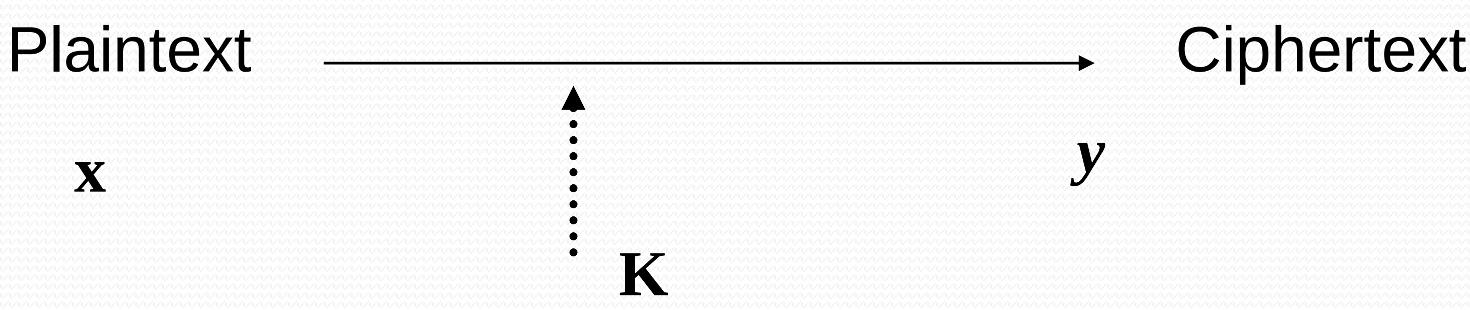
- If Pr[$y$] > 0, then $$\Pr[x \mid y] = \frac{\Pr[x]\Pr[y \mid x]}{\Pr[y]}$$
- Ex. Let **X** denote the sum of two dice.

  **Y** is a random variable on {$D$, $N$}, **Y**=$D$ if the two dice are the same. (double)

$$\Pr[D \mid 4] = \frac{\Pr[4 \mid D]\Pr[D]}{\Pr[4]} = \frac{(1/6)(1/6)}{3/36} = \frac{1}{3}$$

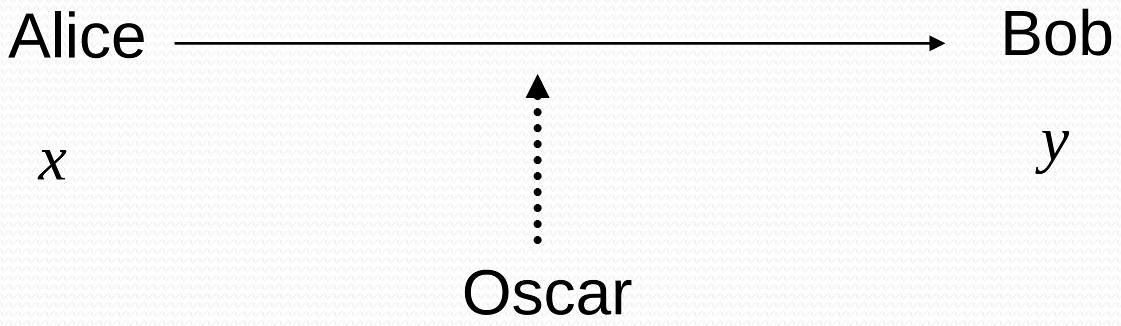
# Definitions

- Assume a cryptosystem (P,C,K,E,D) is specified, and a key is used for one encryption
- Plaintext is denoted by random variable **x**
- Key is denoted by random variable **K**
- Ciphertext is denoted by random variable **y**



# Perfect secrecy

- **Definition:** A cryptosystem has perfect secrecy if $\Pr[x|y] = \Pr[x]$ for all $x \in P$, $y \in C$
- Idea: Oscar can obtain no information about the plaintext by observing the ciphertext



# Relations among **x, K, y**

- Ciphertext is a function of **x** and **K**

$$\Pr[\mathbf{y} = y] = \sum_{\{K: y \in C(K)\}} \Pr[\mathbf{K} = K] \Pr[\mathbf{x} = d_K(y)]$$

- **y** is the ciphertext, given that **x** is the plaintext

$$\Pr[\mathbf{y} = y \mid \mathbf{x} = x] = \sum_{\{K: x = d_K(y)\}} \Pr[\mathbf{K} = K]$$

# Relations among **x, K, y**

- **x** is the plaintext, given that **y** is the ciphertext

$$\Pr[\mathbf{x}=x \mid \mathbf{y}=y] = \frac{\Pr[x]\Pr[y \mid x]}{\Pr[y]}$$

$$= \frac{\Pr[\mathbf{x}=x] \times \sum_{\{K: x=d_K(y)\}} \Pr[\mathbf{K}=K]}{\sum_{\{K: y \in C(K)\}} \Pr[\mathbf{K}=K]\Pr[\mathbf{x}=d_K(y)]}$$

# Ex. Shift cipher has perfect secrecy

- Shift cipher: P=C=K=$Z_{26}$ , encryption is defined as

$$e_K(x) = (x + K) \mod 26$$

- Ciphertext:

$$\Pr[\mathbf{y} = y] = \sum_{K \in Z_{26}} \Pr[\mathbf{K} = K] \Pr[\mathbf{x} = d_K(y)]$$

$$= \sum_{K \in Z_{26}} \tfrac{1}{26} \Pr[x = y - K]$$

$$= \tfrac{1}{26} \sum_{K \in Z_{26}} \Pr[x = y - K] = \tfrac{1}{26}$$

# Ex. Shift cipher has perfect secrecy

- $\Pr[y|x]$

$$= \Pr[\mathbf{K} = (y - x) \mod 26] = \tfrac{1}{26}$$

- Apply Bayes' theorem

$$\Pr[x \mid y] = \frac{\Pr[x]\Pr[y \mid x]}{\Pr[y]}$$

$$= \frac{\Pr[x]\tfrac{1}{26}}{\tfrac{1}{26}} = \Pr[x]$$

Perfect secrecy

# Perfect secrecy when |K|=|C|=|P|

- (P,C,K,E,D) is a cryptosystem where |K|=|C|=|P|.
- The cryptosystem provides perfect secrecy iff
  - every keys is used with equal probability 1/|K|
  - For every $x \in P$, $y \in C$, there is a unique key K such that

Ex. One-time pad in $Z_2$

$$e_K(x) = y$$

# Shannon’s Product Ciphers and Modern Encryption Algorithms

# Product Cryptosystems

- Different cryptosystems can be combined to create a new cryptosystem.
- Given two cryptosystems with the same message space, consider a probabilistic combination of the two systems: with probability $p$ use system A, otherwise use system B.

# Product Cryptosystems

- Another way to use two cryptosystems is to encrypt and decrypt messages consecutively. We call this a **product cipher**.
- He believes that a combination of an initial transposition (Permutation) with alternating substitutions and linear operations may do the trick.
- Both DES and AES use Shannon’s ideas of Product System and of type Substitution Permutation Network (SPN).

# Conventional Encryption Principles

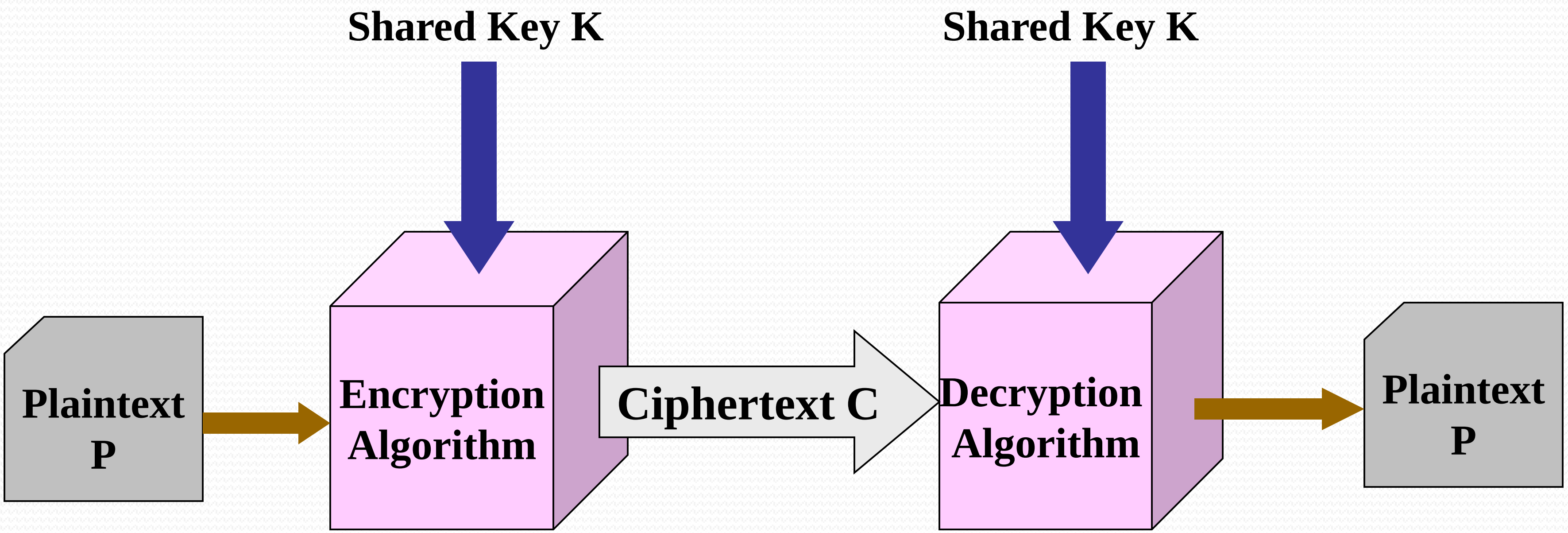
- Basic ingredients of the scheme:
  a) Plaintext (P)
     - Message to be encrypted
  b) Secret Key (K)
     - Shared among the two parties
  c) Ciphertext (C)
     - Message after encryption
  d) Encryption algorithm
     - Uses P and K
  e) Decryption algorithm
     - Uses C and K

# Types of algorithms

- Private Key : The encryption key and decryption key are easily derivable from each other
  - Block Cipher : Fixed blocks of data
  - Stream Cipher : Block Size = 1
- Public Key : Infeasible to determine the decryption key, d from the encryption key, e.

- Security of the scheme
  - Depends on the secrecy of the key
  - Does not depend on the secrecy of the algorithm
- Assumptions that we make:
  - Algorithms for encryption/decryption are known to the public
  - Keys used are kept secret

# Simplified Model of Encryption/Decryption



# Example

Let P = {a,b} with Pr[a] = ¼, Pr[b] = ¾.

Let K = {k1, k2, k3} with Pr[k1] = ½, Pr[k2] = Pr[k3] = ¼.

Let C= {1, 2, 3, 4} and encryption function is

ek1(a) = 1, ek1(b) = 2,

ek2(a) = 2, ek2(b) = 3,

ek3(a) = 3, ek3(b) = 4,

Pr[1] = 1/8, Pr[2] 7/16, Pr[3] =1/4, Pr[4] = 3/16

Pr[a/1] = 1, Pr[a/2] = 1/7, Pr[a/3] = 1/4, Pr[a/4] = 0,

Pr[b/1] = 0, Pr[b/2] = 6/7, Pr[b/3] = 3/4, Pr[b/4] = 1,