# CS 3002 Information Security

## Fall 2022

1. Explain key concepts of information security such as design principles, cryptography, risk management,(1)

2. Discuss legal, ethical, and professional issues in information security (6)
3. Analyze real world scenarios, model them using security measures, and apply various security and risk management tools for achieving information security and privacy (2)
4. Identify appropriate techniques to tackle and solve problems of real life in the discipline of information security (3)
5. Understand issues related to ethics in the field of information security(8)

ISO/IEC 27001: 2013

Week # 2 – Lecture # 3, 4, 5

2nd , 3rd , 5th Safar ul Muzaffar, 1445

6th , 7th, 9th September 2022

Dr. Nadeem Kafi Khan

# Lecture # 3

- Relationship between security concepts
- Threats consequences and type of Threat actions that cause each
- Scope of Computer Security
- Computer and Network Assets with example of threats
- List of Security design principles
- Computer Security Strategy

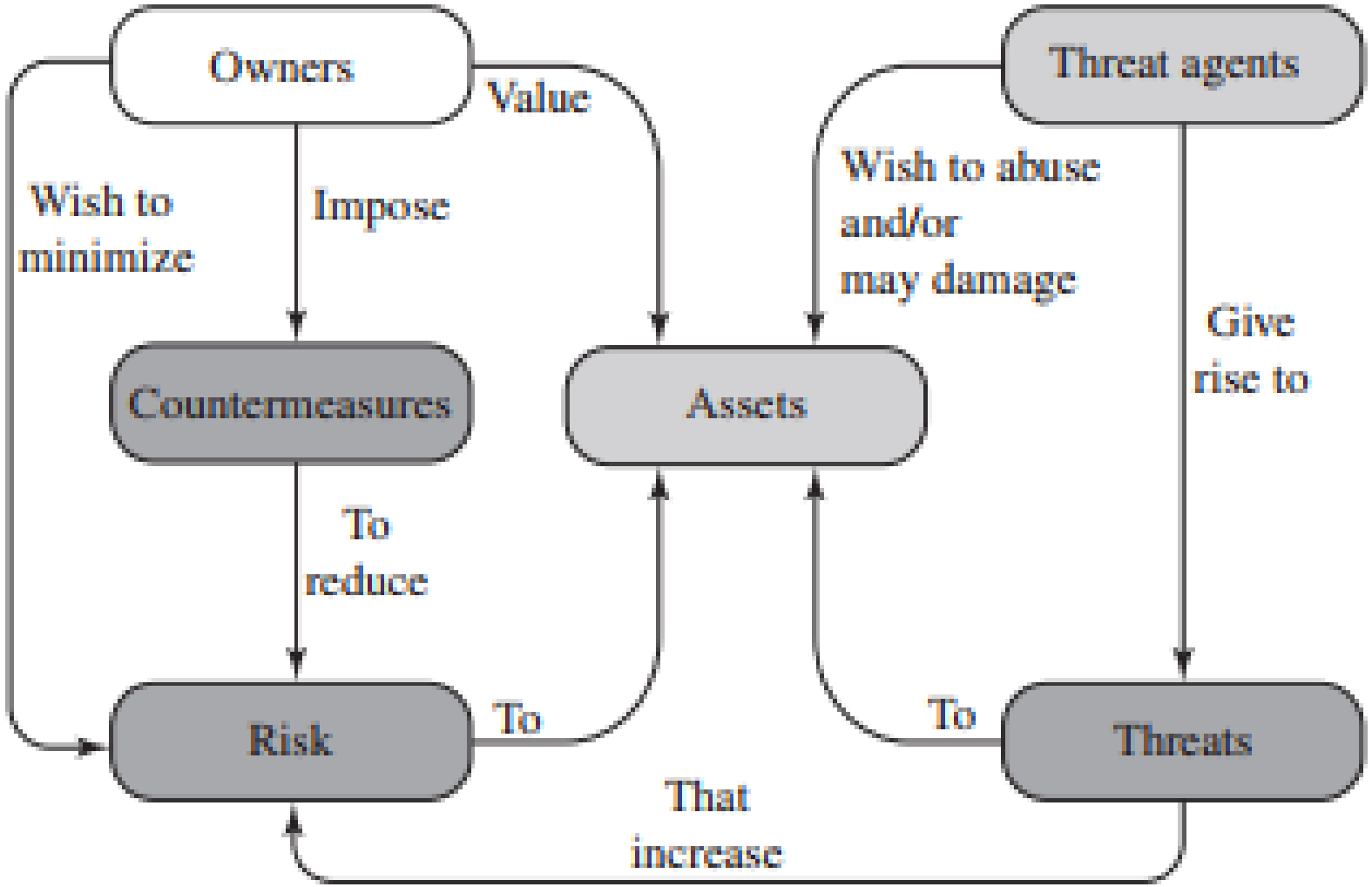



**Figure 1.2 Security Concepts and Relationships**

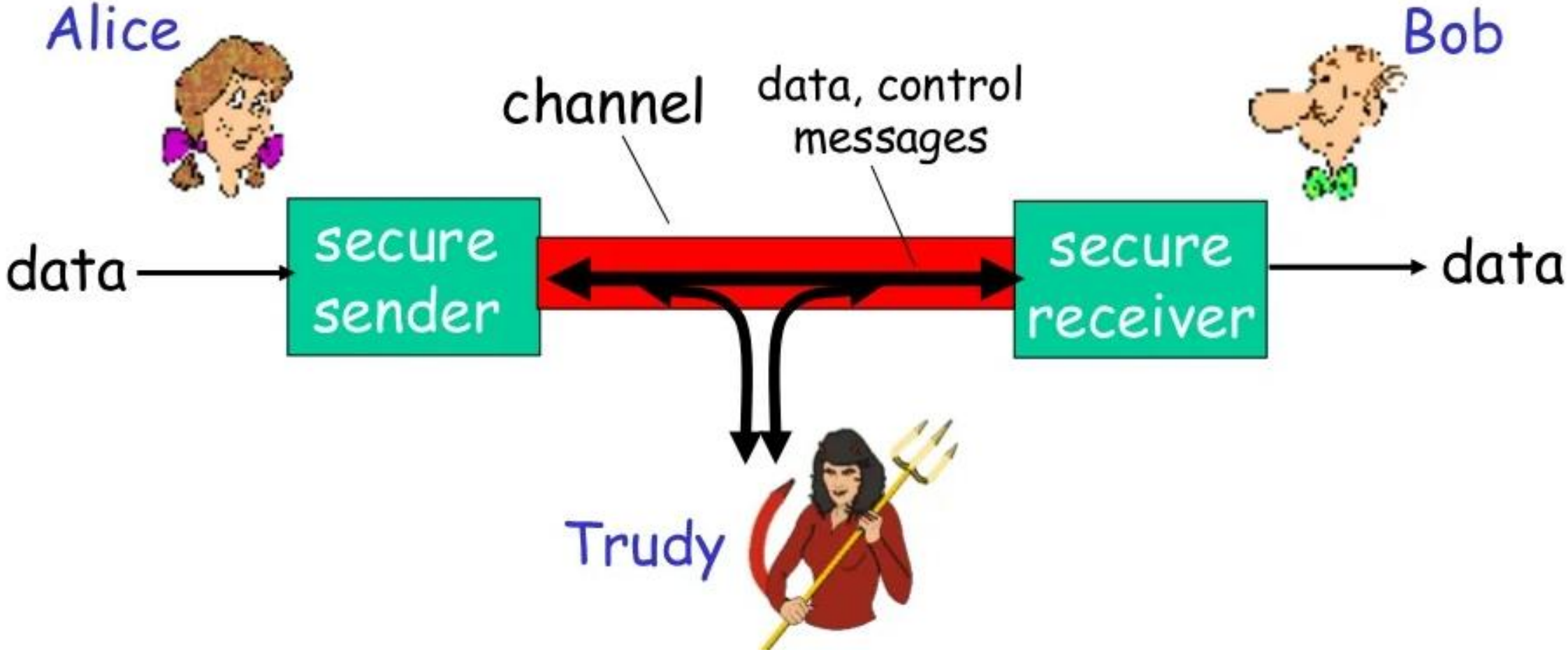

Alice
Bob
channel
data, control
messages
data
secure
sender
secure
receiver
data
Trudy

Table 1.2 **Threat Consequences, and the Types of Threat Actions that Cause Each Consequence**

| Threat Consequence | Threat Action (Attack) |
|---|---|
| **Unauthorized Disclosure**<br>A circumstance or event whereby an entity gains access to data for which the entity is not authorized. | **Exposure:** Sensitive data are directly released to an unauthorized entity.<br>**Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations.<br>**Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications.<br>**Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections. |
| **Deception**<br>A circumstance or event that may result in an authorized entity receiving false data and believing it to be true. | **Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.<br>**Falsification:** False data deceive an authorized entity.<br>**Repudiation:** An entity deceives another by falsely denying responsibility for an act. |
| **Disruption**<br>A circumstance or event that interrupts or prevents the correct operation of system services and functions. | **Incapacitation:** Prevents or interrupts system operation by disabling a system component.<br>**Corruption:** Undesirably alters system operation by adversely modifying system functions or data.<br>**Obstruction:** A threat action that interrupts delivery of system services by hindering system operation. |
| **Usurpation**<br>A circumstance or event that results in control of system services or functions by an unauthorized entity. | **Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource.<br>**Misuse:** Causes a system component to perform a function or service that is detrimental to system security. |

*Source*: Based on RFC 4949

| Threat Consequence | Threat Action (Attack) |
| --- | --- |
| **Unauthorized Disclosure**<br>A circumstance or event whereby an entity gains access to data for which the entity is not authorized. | **Exposure:** Sensitive data are directly released to an unauthorized entity.<br>**Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations.<br>**Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications.<br>**Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections. |

| Threat Consequence | Threat Action (Attack) |
| --- | --- |
| **Deception**<br>A circumstance or event that may result in an authorized entity receiving false data and believing it to be true. | **Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.<br>**Falsification:** False data deceive an authorized entity.<br>**Repudiation:** An entity deceives another by falsely denying responsibility for an act. |

| Threat Consequence | Threat Action (Attack) |
| --- | --- |
| **Disruption**<br>A circumstance or event that interrupts or prevents the correct operation of system services and functions. | **Incapacitation:** Prevents or interrupts system operation by disabling a system component.<br>**Corruption:** Undesirably alters system operation by adversely modifying system functions or data.<br>**Obstruction:** A threat action that interrupts delivery of system services by hindering system operation. |

| Threat Consequence | Threat Action (Attack) |
| --- | --- |
| **Usurpation**<br>A circumstance or event that results in control of system services or functions by an unauthorized entity. | **Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource.<br>**Misuse:** Causes a system component to perform a function or service that is detrimental to system security. |

# Scope of Computer Security

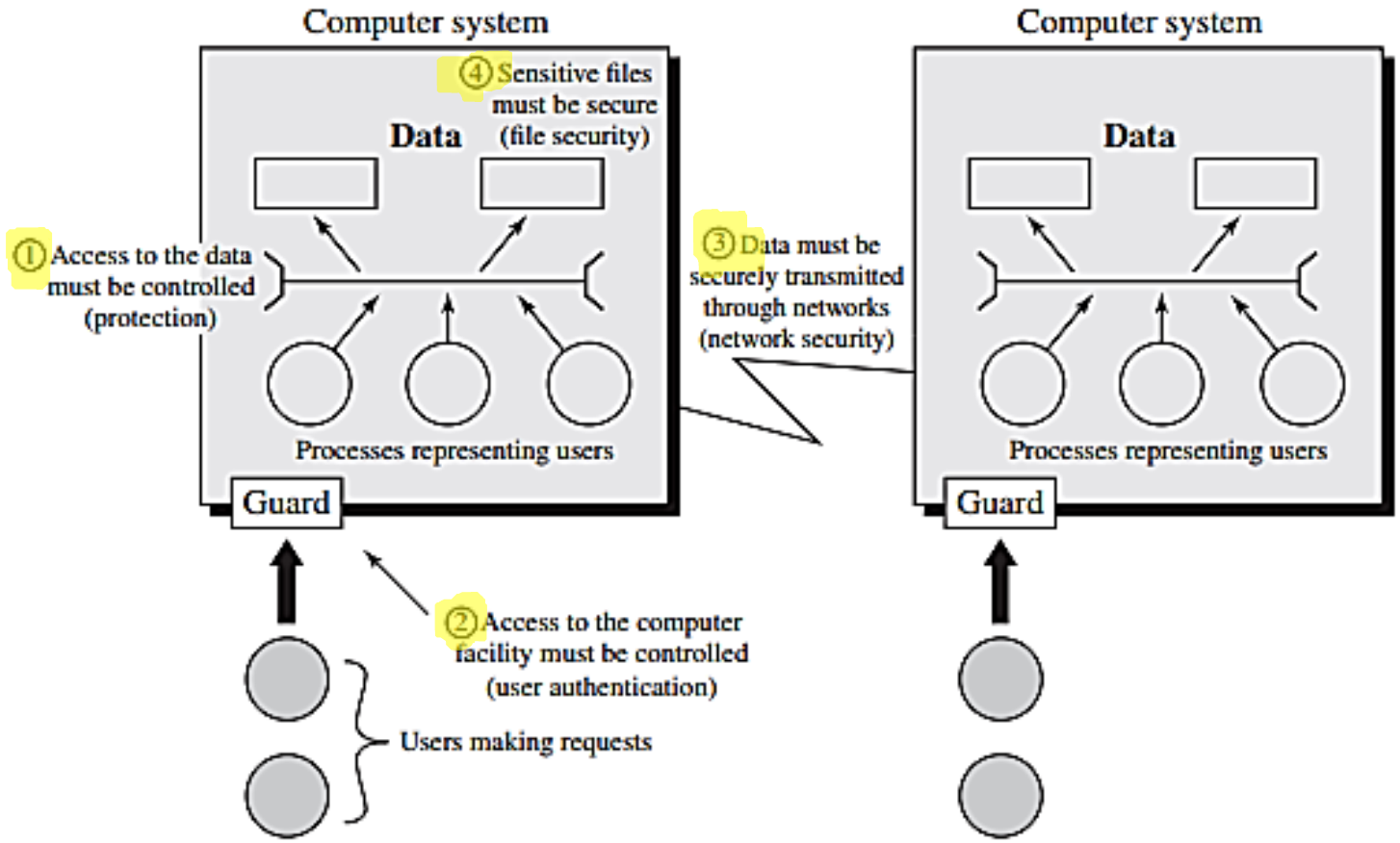



Figure 1.3 **Scope of Computer Security**

*Note*: This figure depicts security concerns other than physical security, including controlling of access to computers systems, safeguarding of data transmitted over communications systems, and safeguarding of stored data.

- [1] Access to the data must be controlled (protection)
- [2] Access to the computer facility must be controlled (user authentication)
- [3] Data must be securely transmitted through networks (network security)
- [4] Sensitive files must be secure (file security)

- **Physical Security**
- **OS Security**
- **Application**
- **Social Engineering**

Table 1.3 **Computer and Network Assets, with Examples of Threats**

| | Availability | Confidentiality | Integrity |
|---|---|---|---|
| **Hardware** | Equipment is stolen or disabled, thus denying service. | An unencrypted USB drive is stolen. | |
| **Software** | Programs are deleted, denying access to users. | An unauthorized copy of software is made. | A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task. |
| **Data** | Files are deleted, denying access to users. | An unauthorized read of data is performed. An analysis of statistical data reveals underlying data. | Existing files are modified or new files are fabricated. |
| **Communication Lines and Networks** | Messages are destroyed or deleted. Communication lines or networks are rendered unavailable. | Messages are read. The traffic pattern of messages is observed. | Messages are modified, delayed, reordered, or duplicated. False messages are fabricated. |

## 1.4 FUNDAMENTAL SECURITY DESIGN PRINCIPLES

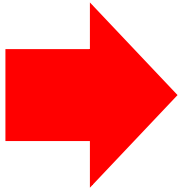
Despite years of research and development, it has not been possible to develop security design and implementation techniques that systematically exclude security flaws and prevent all unauthorized actions. In the absence of such foolproof techniques, it is useful to have a set of widely agreed design principles that can guide the development of protection mechanisms. The National Centers of Academic Excellence in Information Assurance/Cyber Defense, which is jointly sponsored by the U.S. National Security Agency and the U. S. Department of Homeland Security, list the following as fundamental security design principles [NCAE13]:

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability
- Isolation
- Encapsulation
- Modularity
- Layering
- Least astonishment

# 1.6 COMPUTER SECURITY STRATEGY

We conclude this chapter with a brief look at the overall strategy for providing computer security. [LAMP04] suggests that a comprehensive security strategy involves three aspects:

- **Specification/policy:** What is the security scheme supposed to do?
- **Implementation/mechanisms:** How does it do it?
- **Correctness/assurance:** Does it really work?



ISO 9001:2015 employs the process approach, which incorporates the Plan-Do-Check-Act (PDCA) cycle and risk-based thinking. This means the organisation needs to:

1. determine required process inputs and expected outputs
2. assign responsibilities and authorities for processes
3. identify risks and opportunities for processes, and plan to address these

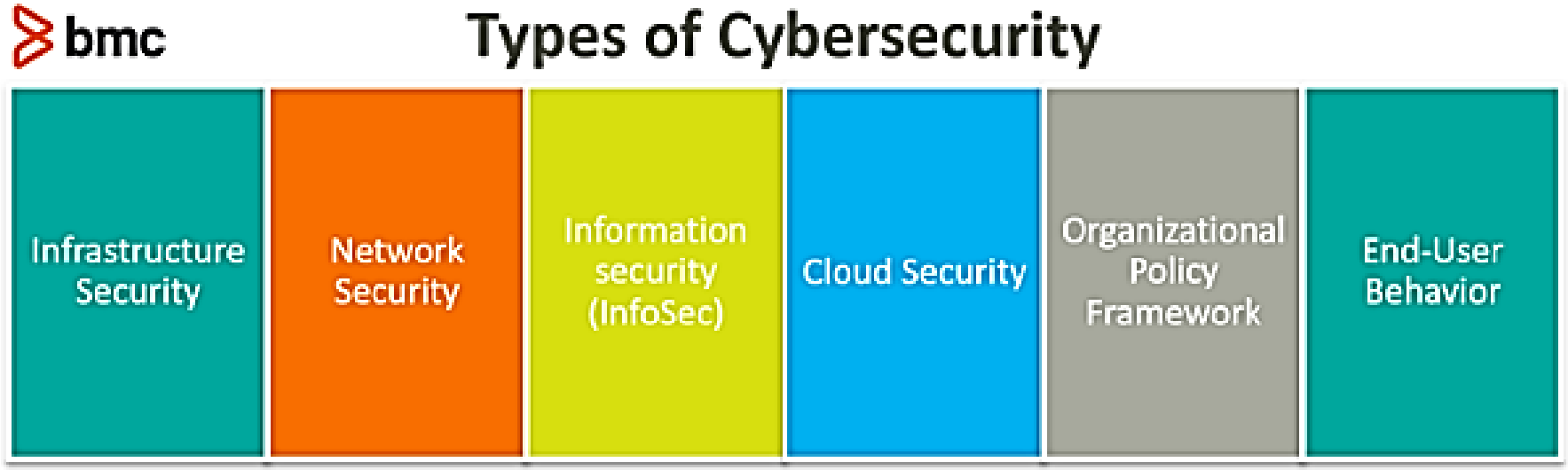
# 1.7 STANDARDS

- **National Institute of Standards and Technology:** NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private sector innovation. Despite its national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact.

- **ITU-T:** The International Telecommunication Union (ITU) is a United Nations agency in which governments and the private sector coordinate global telecom networks and services. The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors of the ITU. ITU-T's mission is the production of standards covering all fields of telecommunications. ITU-T standards are referred to as Recommendations.

- **Internet Society:** ISOC is a professional membership society with worldwide organizational and individual membership. It provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). These organizations develop Internet standards and related specifications, all of which are published as Requests for Comments (RFCs).

- **ISO:** The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from more than 140 countries. ISO is a nongovernmental organization that promotes the development of standardization and related activities with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity. ISO's work results in international agreements that are published as International Standards.

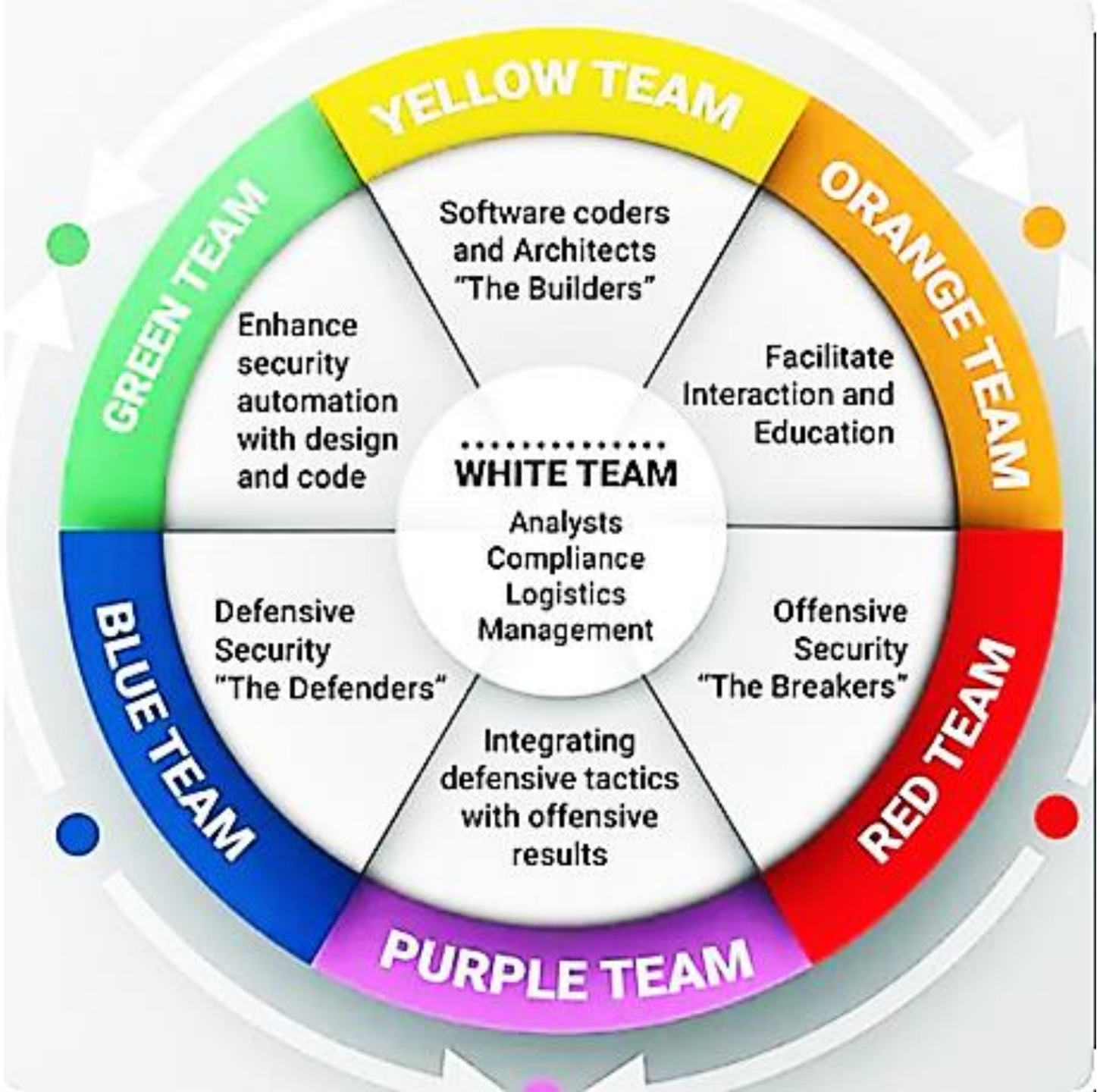



- Physical Security
- Access Security of Infrastructure
- Information security (including non digital)
- OS security
- Application Security
- Network Security

- Identification of Assets
- Identify Vulnerabilities
  - (CIA + Authentication + Auditable)
- Risk Assessment → Possible Threats
- Known and possible Attacks
- Test and Implement known Countermeasures
  - Based on community Best Practices
- Governmental and Community based efforts
  - Groups (Meetups) + CERTs + Conferences + Certifications

# InfoSec Practice

- Identification of Assets
- Identify Vulnerabilities
  - (CIA + Authentication + Auditable)
- Risk Assessment → Possible Threats
- Known and possible Attacks
- Test and Implement known Countermeasures
  - Based on community Best Practices
- Governmental and Community based efforts
  - Groups (Meetups) + CERTs + Conferences + Certifications


YELLOW TEAM
ORANGE TEAM
GREEN TEAM
BLUE TEAM
RED TEAM
PURPLE TEAM
Software coders and Architects "The Builders"
Enhance security automation with design and code
Facilitate Interaction and Education
WHITE TEAM
Analysts
Compliance
Logistics
Management
Defensive Security "The Defenders"
Offensive Security "The Breakers"
Integrating defensive tactics with offensive results

# Lecture # 4

- Symmetric Encryption and Decryption
  - Definition
  - Model
  - Vocabulary
  - Two requirements for secure use of Symmetric Encryption/Decryption
  - Attacking a Symmetric Encryption Scheme
    - Brute-force Attack
    - Cryptanalysis

# Possible Coverage before Midterm # 1

Topics from Chapter # 2, Chapter # 20 and Chapter # 21

2.1 **Confidentiality with Symmetric Encryption**

- Symmetric Encryption
- Symmetric Block Encryption Algorithms
- Stream Ciphers

2.2 **Message Authentication and Hash Functions**

- Authentication Using Symmetric Encryption
- Message Authentication without Message Encryption
- Secure Hash Functions
- Other Applications of Hash Functions

2.3 **Public-Key Encryption**

- Public-Key Encryption Structure
- Applications for Public-Key Cryptosystems
- Requirements for Public-Key Cryptography
- Asymmetric Encryption Algorithms

2.4 **Digital Signatures and Key Management**

- Digital Signature
- Public-Key Certificates
- Symmetric Key Exchange Using Public-Key Encryption
- Digital Envelopes

20.2 **Data Encryption Standard**

- Data Encryption Standard
- Triple DES

20.3 **Advanced Encryption Standard**

- Overview of the Algorithm
- Algorithm Details

21.4 **The RSA Public-Key Encryption Algorithm**

- Description of the Algorithm
- The Security of RSA

CHAPTER 2

# CRYPTOGRAPHIC TOOLS

## 2.1 Confidentiality with Symmetric Encryption

Symmetric Encryption
Symmetric Block Encryption Algorithms
Stream Ciphers

## 2.1 CONFIDENTIALITY WITH SYMMETRIC ENCRYPTION

Encryption is the process of converting information or data into a code, especially to prevent unauthorized access.

### Symmetric Encryption

Symmetric encryption, also referred to as conventional encryption or single-key encryption, was the only type of encryption in use prior to the introduction of public-key encryption in the late 1970s. Countless individuals and groups, from Julius Caesar to the German U-boat force to present-day diplomatic, military, and commercial users, have used symmetric encryption for secret communication. It remains the more widely used of the two types of encryption.

## 2.1 CONFIDENTIALITY WITH SYMMETRIC ENCRYPTION

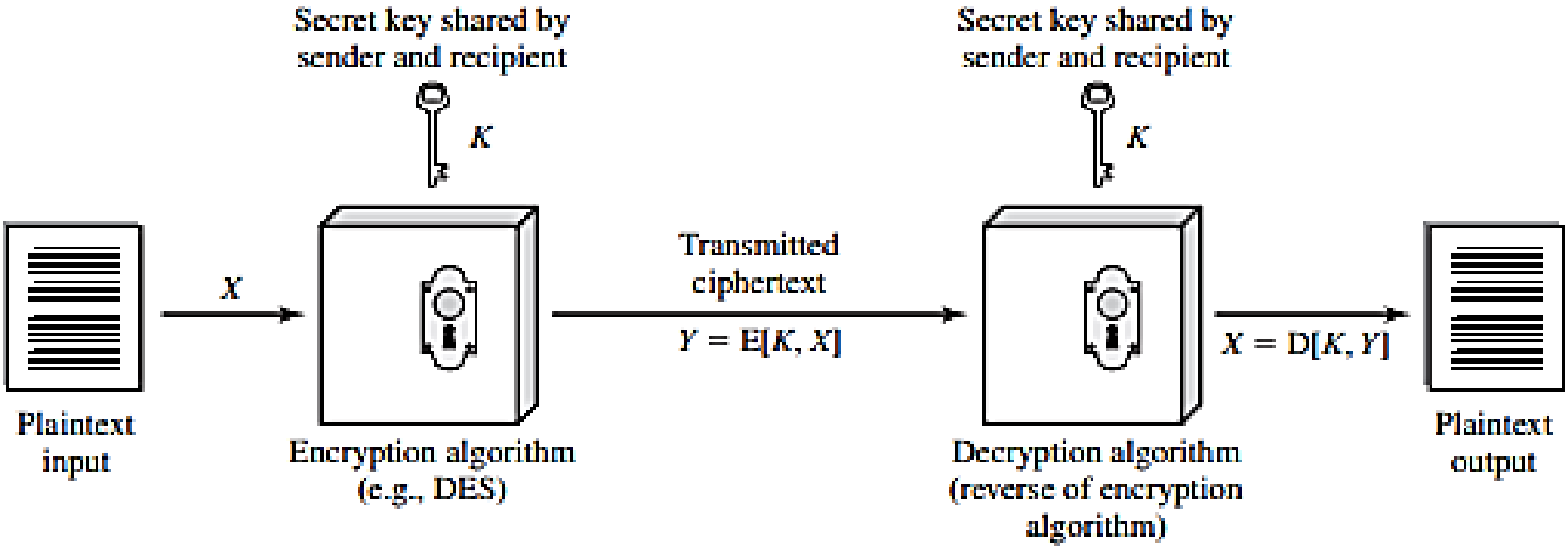



**Figure 2.1 Simplified Model of Symmetric Encryption**

## 2.1 CONFIDENTIALITY WITH SYMMETRIC ENCRYPTION

A symmetric encryption scheme has five ingredients (see Figure 2.1):

- **Plaintext:** This is the original message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

## 2.1 CONFIDENTIALITY WITH SYMMETRIC ENCRYPTION

There are two requirements for secure use of symmetric encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form: The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.
2. The sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

# Attacking a Symmetric Encryption Scheme (1)

- **Brute-force attack** is to try every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained.
  - On average, half of all possible keys must be tried to achieve success. That is, if there are *x* different keys, on average an attacker would discover the actual key after *x*/2 tries.
  - This means size of key has a great impact of breaking the symmetric Encryption schedule. Larger the key the more time it will takes to try all possible key combinations.

Table 2.2 **Average Time Required for Exhaustive Key Search**

| Key Size (bits) | Cipher | Number of Alternative Keys | Time Required at $10^9$ decryptions/$\mu$s | Time Required at $10^{13}$ decryptions/$\mu$s |
|---|---|---|---|---|
| 56 | DES | $2^{56} \approx 7.2 \times 10^{16}$ | $2^{55}\ \mu s = 1.125$ years | 1 hour |
| 128 | AES | $2^{128} \approx 3.4 \times 10^{38}$ | $2^{127}\ \mu s = 5.3 \times 10^{21}$ years | $5.3 \times 10^{17}$ years |
| 168 | Triple DES | $2^{168} \approx 3.7 \times 10^{50}$ | $2^{167}\ \mu s = 5.8 \times 10^{33}$ years | $5.8 \times 10^{29}$ years |
| 192 | AES | $2^{192} \approx 6.3 \times 10^{57}$ | $2^{191}\ \mu s = 9.8 \times 10^{40}$ years | $9.8 \times 10^{36}$ years |
| 256 | AES | $2^{256} \approx 1.2 \times 10^{77}$ | $2^{255}\ \mu s = 1.8 \times 10^{60}$ years | $1.8 \times 10^{56}$ years |

# Attacking a Symmetric Encryption Scheme (1)

- **Brute-force attack** is to try every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained.
  - On average, half of all possible keys must be tried to achieve success. That is, if there are *x* different keys, on average an attacker would discover the actual key after *x*/2 tries.
  - This means size of key has a great impact of breaking the symmetric Encryption schedule. Larger the key the more time it will takes to try all possible key combinations.
- More information about plain text is needed **to break in less time** (i.e. trying half the keys):
  - Language of the plain text. This make it easy to recognize the result.
  - If the text message has been compressed before encryption, then recognition is more difficult.
  - A numerical file that has been compressed, the problem becomes even more difficult.

# Attacking a Symmetric Encryption Scheme (2)

- **Cryptanalysis**. Cryptanalysis refers to the process of analyzing information systems in order to understand hidden aspects of the systems.

- Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

- This attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of
  - the plaintext, or
  - some knowledge of some plaintext-ciphertext pairs.

- This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used. If the attack succeeds in deducing the key, the effect is catastrophic: All future and past messages encrypted with that key are compromised.

# Lecture # 5

- Types of Symmetric Encryption
  - Block Ciphers
  - Stream Ciphers
- Symmetric Block Encryption Algorithms
  - DES and AES
  - Weaknesses of DES and Triple-DES
- Data Encryption Standard (DES) Algorithms

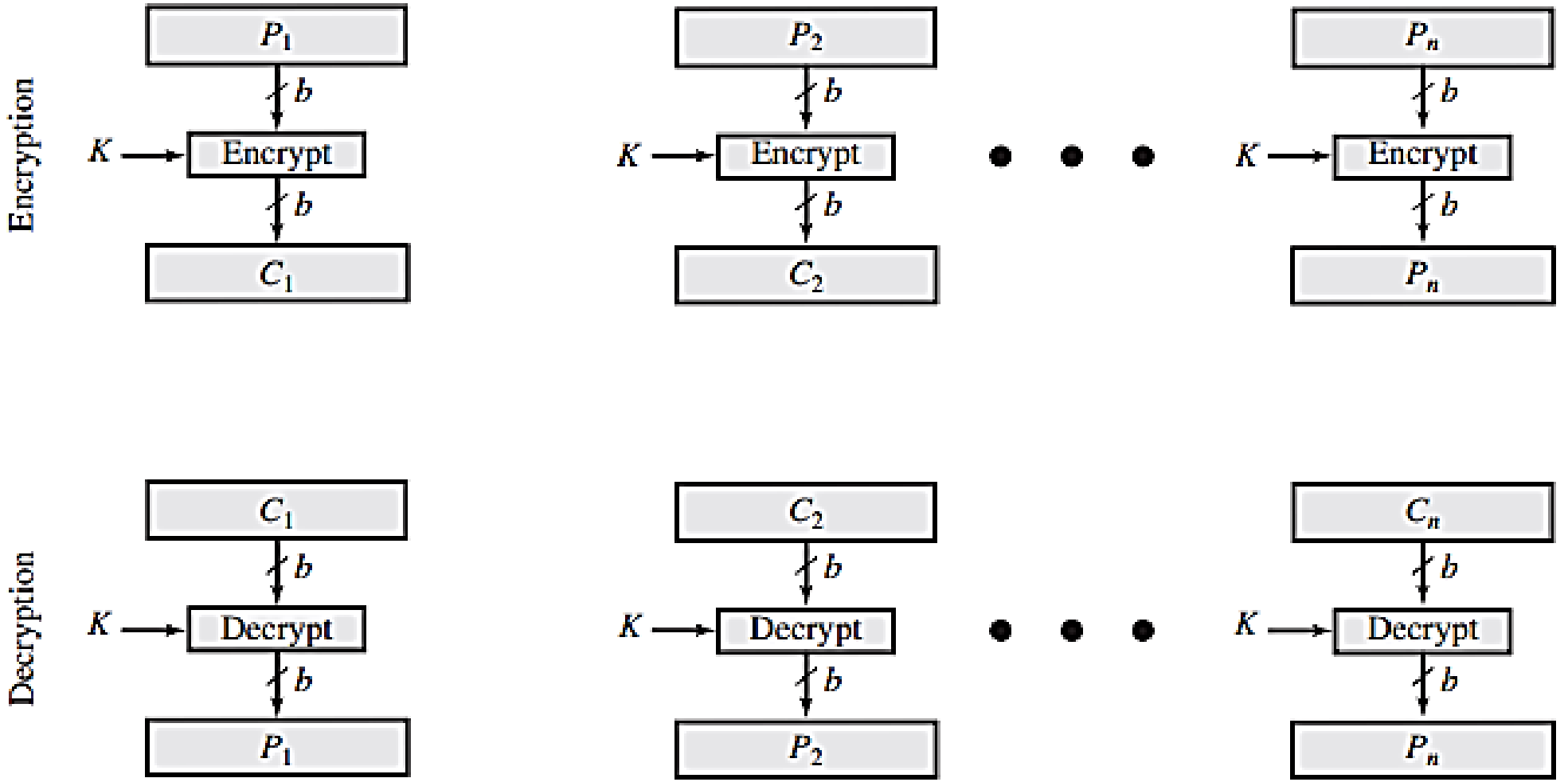
# Types of Symmetric Encryption

## Symmetric Block Encryption Algorithms

The most commonly used symmetric encryption algorithms are block ciphers. A block cipher processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block. The algorithm processes longer plaintext amounts as a series of fixed-size blocks. The most important symmetric algo-

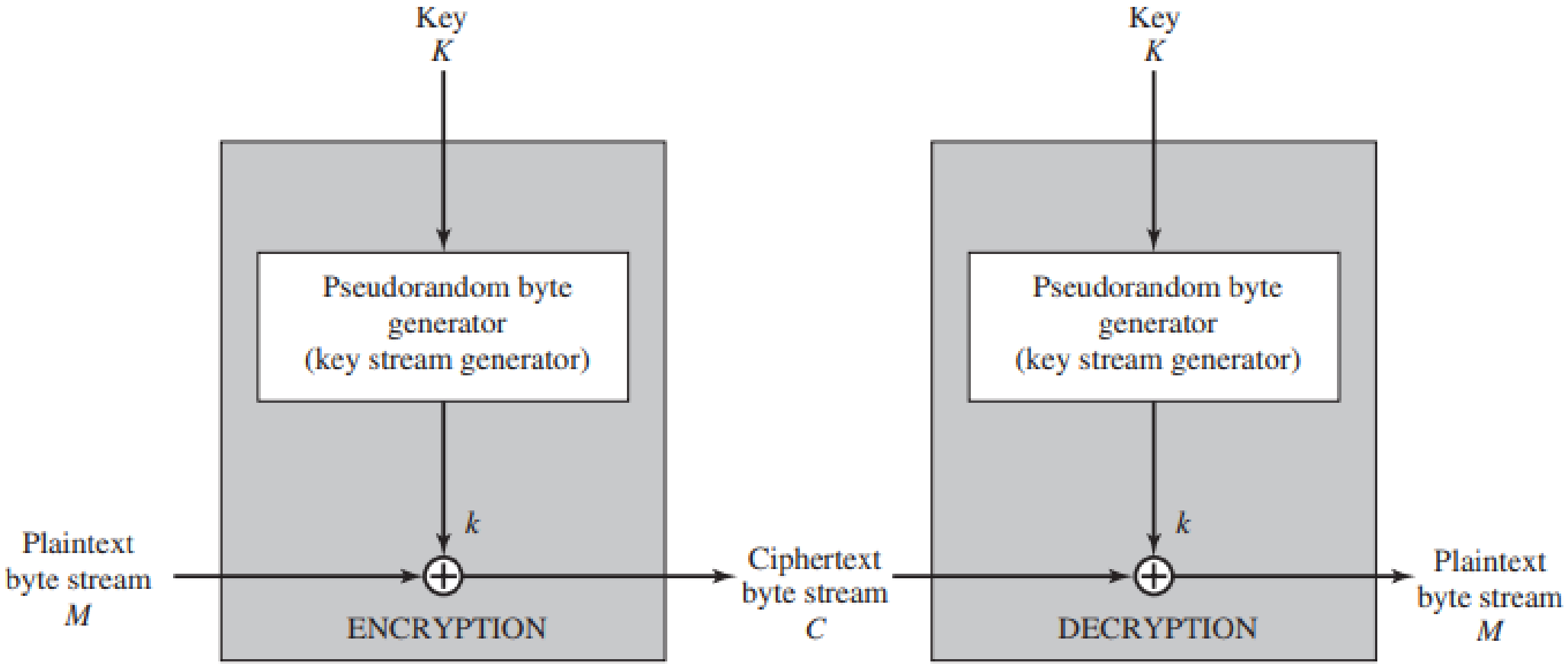
## Stream Ciphers

A *block cipher* processes the input one block of elements at a time, producing an output block for each input block. A *stream cipher* processes the input elements continuously, producing output one element at a time, as it goes along. Although block ciphers are far more common, there are certain applications in which a stream cipher is more appropriate.




(a) Block cipher encryption (electronic codebook mode)

**Figure 2.2 Types of Symmetric Encryption**




(b) Stream encryption

**Figure 2.2 Types of Symmetric Encryption**

# Symmetric Block Encryption Algorithms

The most important symmetric algorithms, all of which are block ciphers, are the Data Encryption Standard (DES), triple DES, and the Advanced Encryption Standard (AES); see Table 2.1. This subsection provides an overview of these algorithms.

Table 2.1 **Comparison of Three Popular Symmetric Encryption Algorithms**

| | DES | Triple DES | AES |
|---|---|---|---|
| **Plaintext block size (bits)** | 64 | 64 | 128 |
| **Ciphertext block size (bits)** | 64 | 64 | 128 |
| **Key size (bits)** | 56 | 112 or 168 | 128, 192, or 256 |

DES = Data Encryption Standard
AES = Advanced Encryption Standard

# Concerns about the strength of DES Algorithm (1)

Concerns about the strength of DES fall into two categories: concerns about the algorithm itself, and concerns about the use of a 56-bit key. The first concern refers to the possibility that cryptanalysis is possible by exploiting the characteristics of the DES algorithm. Over the years, there have been numerous attempts to find and exploit weaknesses in the algorithm, making DES the most-studied encryption algorithm in existence. Despite numerous approaches, no one has so far reported a fatal weakness in DES.

A more serious concern is key length. With a key length of 56 bits, there are $2^{56}$ possible keys, which is approximately $7.2 \times 10^{16}$ keys. Given the speed of commercial off-the-shelf processors, this key length is woefully inadequate. A paper from Seagate Technology [SEAG08] suggests that a rate of one billion ($10^9$) key combinations per second is reasonable for today's multicore computers. Recent offerings confirm this.

# Concerns about the strength of DES Algorithm (2)

Both Intel and AMD now offer hardware-based instructions to accelerate the use of AES. Tests run on a contemporary multicore Intel machine resulted in an encryption rate of about half a billion encryptions per second [BASU12]. Another recent analysis suggests that with contemporary supercomputer technology, a rate of $10^{13}$ encryptions/s is reasonable [AROR12].

Table 2.2 **Average Time Required for Exhaustive Key Search**

| Key Size (bits) | Cipher | Number of Alternative Keys | Time Required at $10^9$ decryptions/$\mu$s | Time Required at $10^{13}$ decryptions/$\mu$s |
|---|---|---|---|---|
| 56 | DES | $2^{56} \approx 7.2 \times 10^{16}$ | $2^{55}\ \mu s = 1.125$ years | 1 hour |
| 128 | AES | $2^{128} \approx 3.4 \times 10^{38}$ | $2^{127}\ \mu s = 5.3 \times 10^{21}$ years | $5.3 \times 10^{17}$ years |
| 168 | Triple DES | $2^{168} \approx 3.7 \times 10^{50}$ | $2^{167}\ \mu s = 5.8 \times 10^{33}$ years | $5.8 \times 10^{29}$ years |
| 192 | AES | $2^{192} \approx 6.3 \times 10^{57}$ | $2^{191}\ \mu s = 9.8 \times 10^{40}$ years | $9.8 \times 10^{36}$ years |
| 256 | AES | $2^{256} \approx 1.2 \times 10^{77}$ | $2^{255}\ \mu s = 1.8 \times 10^{60}$ years | $1.8 \times 10^{56}$ years |

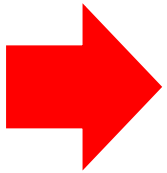
# Addressing the small key size of DES Algorithm

***TRIPLE DES*** The life of DES was extended by the use of triple DES (3DES), which involves repeating the basic DES algorithm three times, using either two or three unique keys, for a key size of 112 or 168 bits.

3DES has two attractions that assure its widespread use over the next few years. First, with its 168-bit key length, it overcomes the vulnerability to brute-force attack of DES. Second, the underlying encryption algorithm in 3DES is the same as in DES. This algorithm has been subjected to more scrutiny than any other encryption algorithm over a longer period of time, and no effective cryptanalytic attack based on the algorithm rather than brute force has been found. Accordingly, there is a high level of confidence that 3DES is very resistant to cryptanalysis. If security were the only consideration, then 3DES would be an appropriate choice for a standardized encryption algorithm for decades to come.

# Drawback of DES Algorithm

The principal drawback of 3DES is that the algorithm is relatively sluggish in software. The original DES was designed for mid-1970s hardware implementation and does not produce efficient software code. 3DES, which requires three times as many calculations as DES, is correspondingly slower. A secondary drawback is that both DES and 3DES use a 64-bit block size. For reasons of both efficiency and security, a larger block size is desirable.



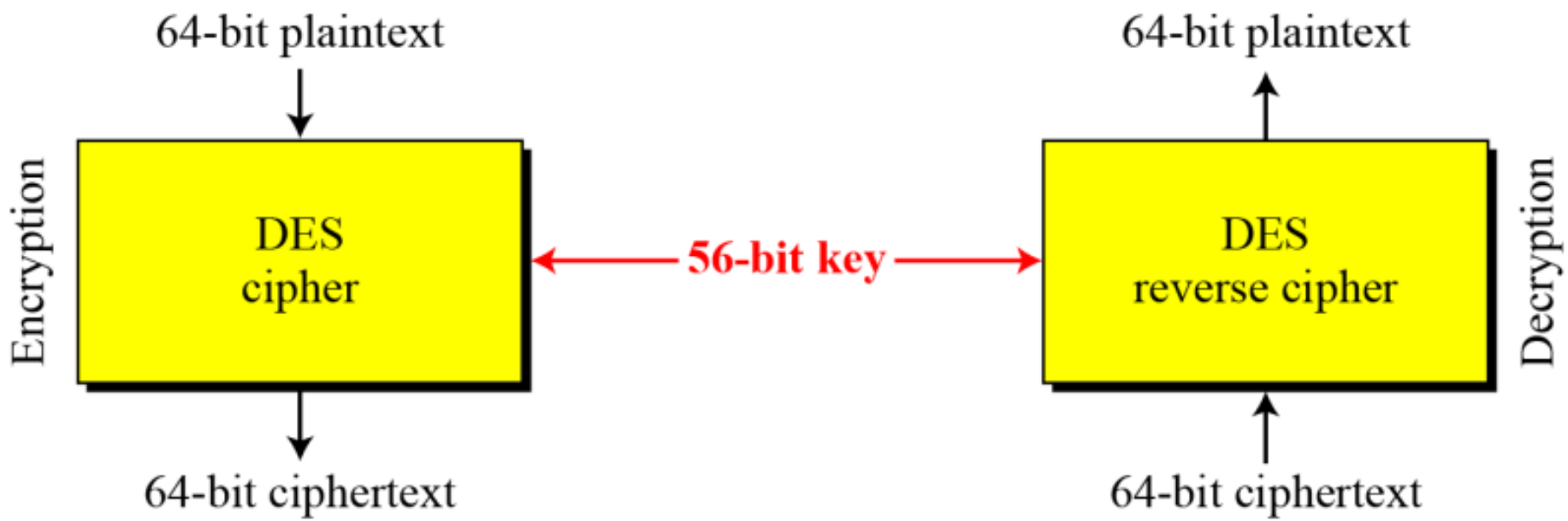
*ADVANCED ENCRYPTION STANDARD* Because of its drawbacks, 3DES is not a reasonable candidate for long-term use. As a replacement, NIST in 1997 issued a call for proposals for a new Advanced Encryption Standard (AES), which should have a security strength equal to or better than 3DES and significantly improved efficiency. In addition to these general requirements, NIST specified that AES must be a symmetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits. Evaluation criteria included security, computational efficiency, memory requirements, hardware and software suitability, and flexibility.

# Data Encryption Standard (DES)

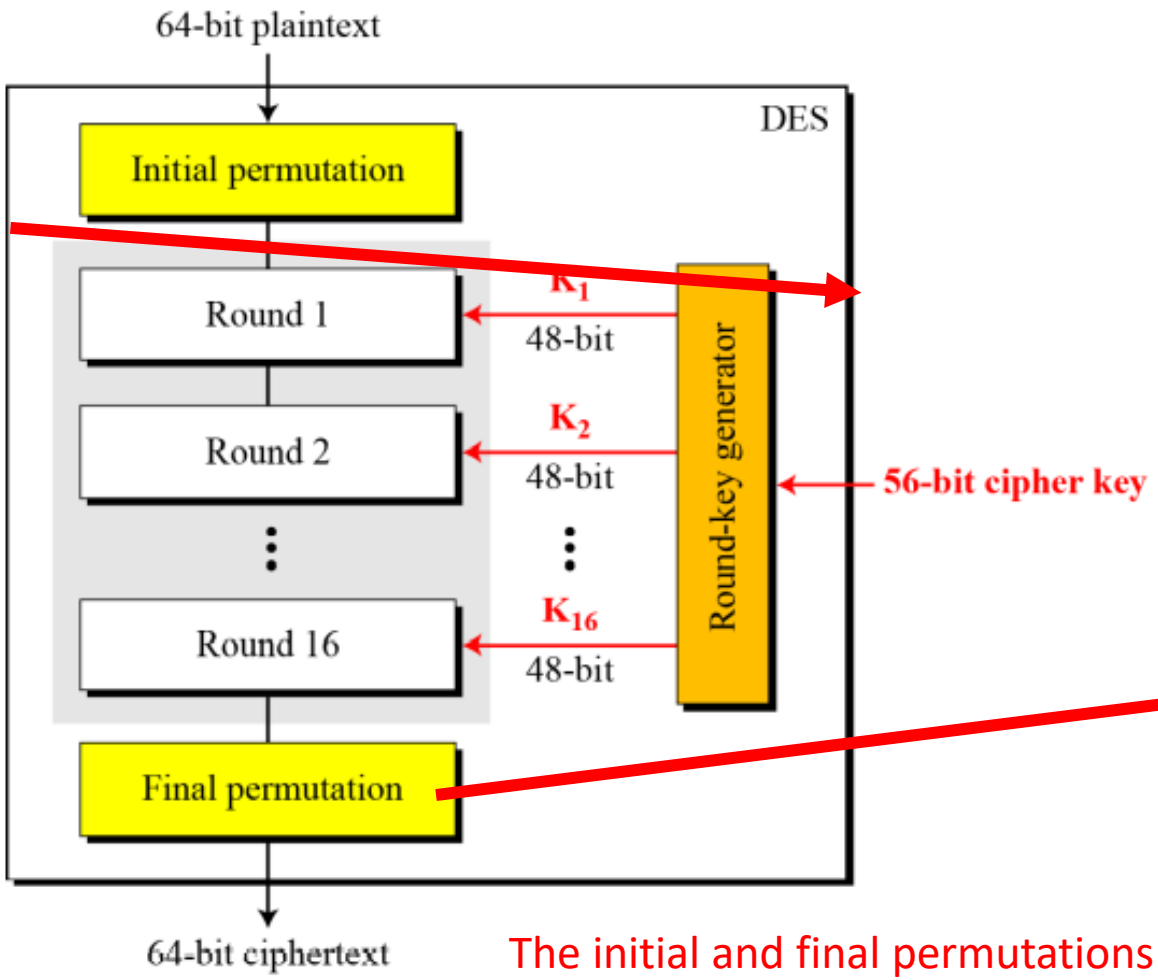
**Coverage from slides provided by Course Coordinator**

***DES is a block cipher, as shown in Figure 6.1.***

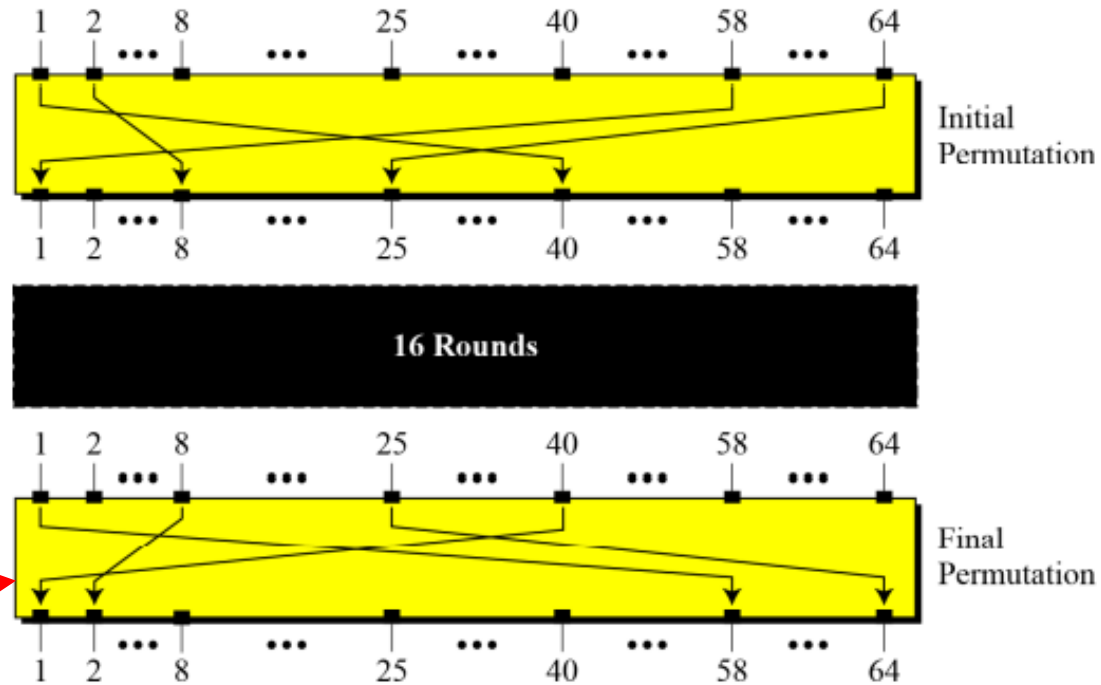
**Figure 6.1** ***Encryption and decryption with DES***



## Figure 6.2 *General structure of DES*




## Figure 6.3 *Initial and final permutation steps in DES*




The initial and final permutations are straight P-boxes that are inverses of each other. They have no cryptography significance in DES.

***DES uses 16 rounds. Each round of DES is a Feistel cipher.***

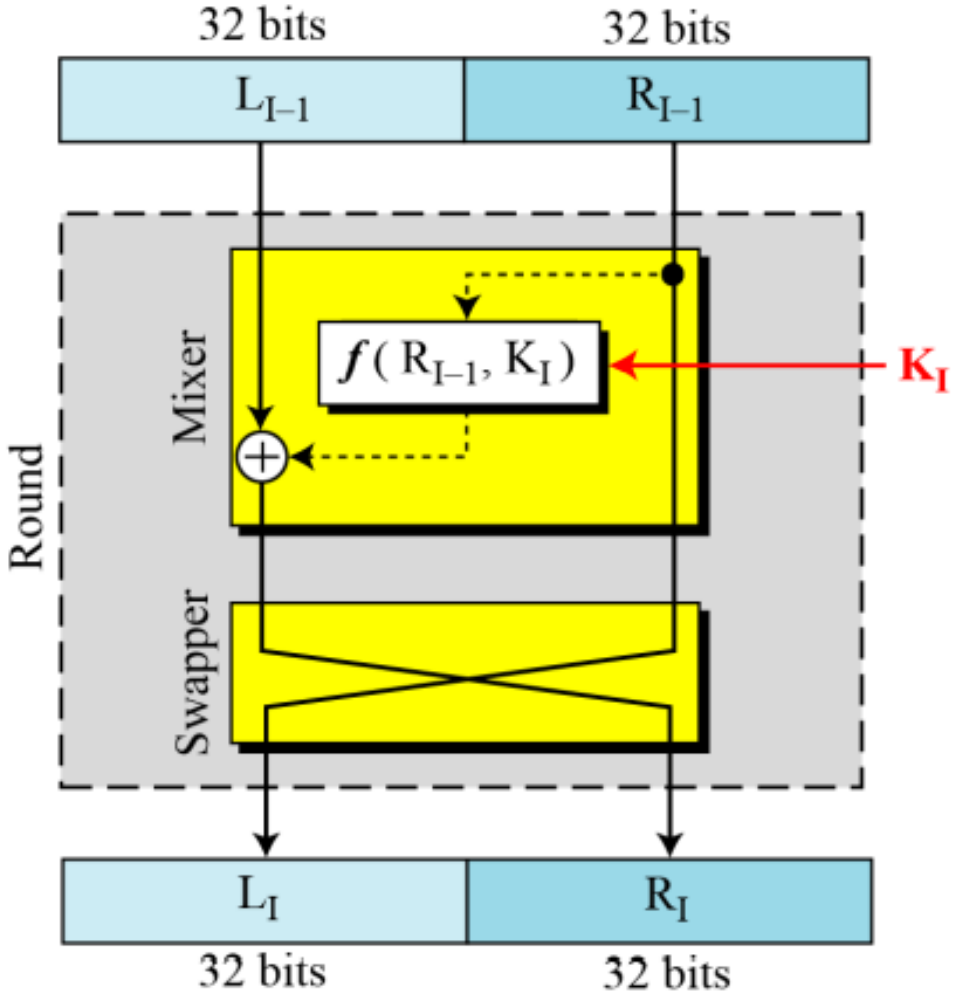



**Figure 6.4**
***A round in DES (encryption site)***

***The heart of DES is the DES function. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.***

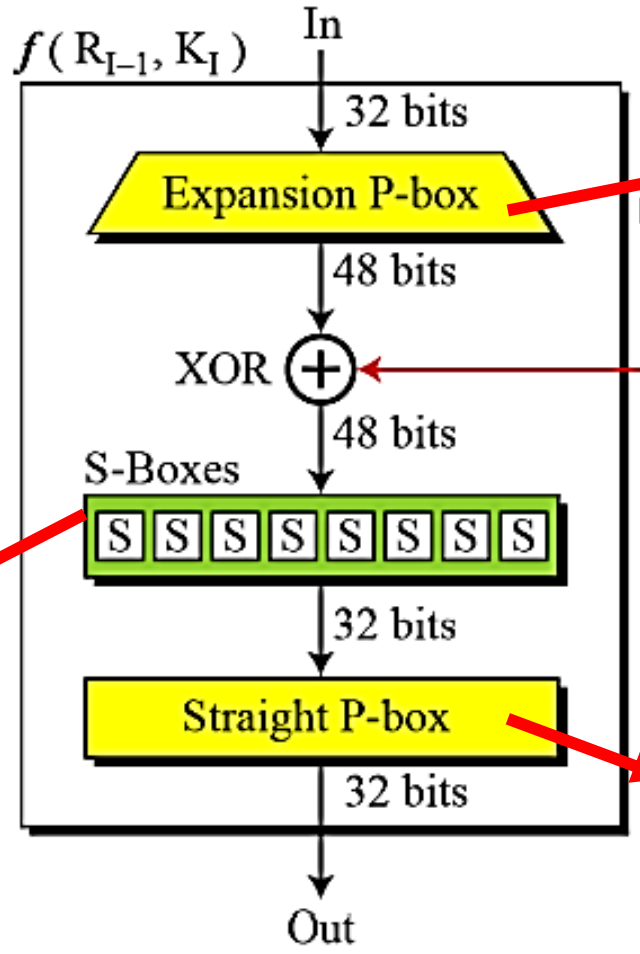
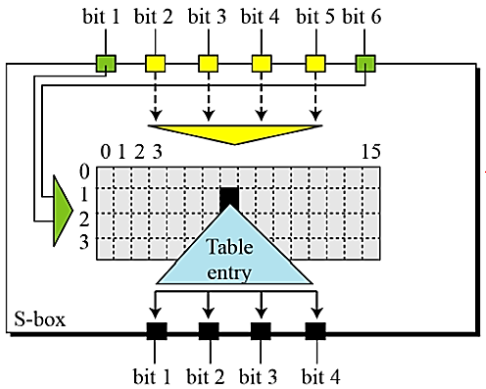



**Figure 6.5**
***DES function***

By duplicating bits

$K_I$ (48 bits)




Details on next slide

**Table 6.6** ***Expansion P-box table***

| | | | | | |
|---|---|---|---|---|---|
| 32 | 01 | 02 | 03 | 04 | 05 |
| 04 | 05 | 06 | 07 | 08 | 09 |
| 08 | 09 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 31 | 31 | 32 | 01 |

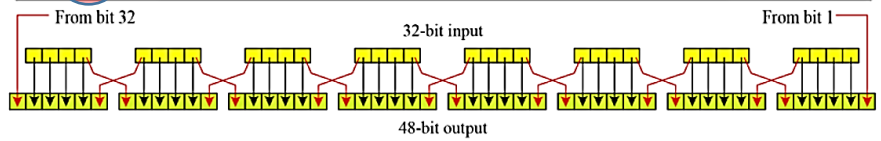



**Table 6.11** ***Straight permutation table***

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16 | 07 | 20 | 21 | 29 | 12 | 28 | 17 |
| 01 | 15 | 23 | 26 | 05 | 18 | 31 | 10 |
| 02 | 08 | 24 | 14 | 32 | 27 | 03 | 09 |
| 19 | 13 | 30 | 06 | 22 | 11 | 04 | 25 |

## *S-Boxes* (Substitution Boxes)

***The S-boxes do the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. See Figure 6.7.***

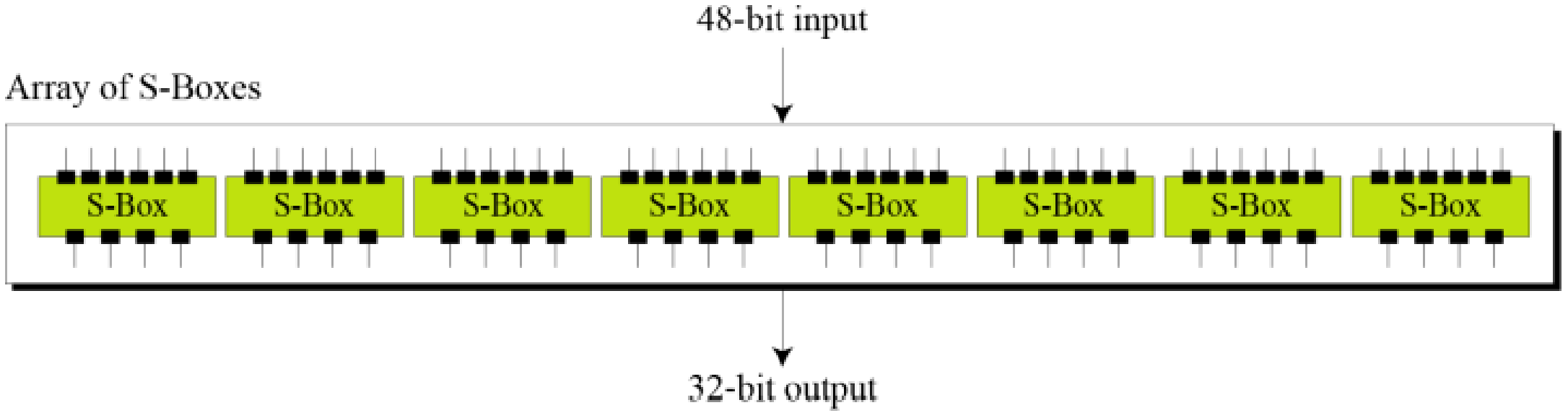
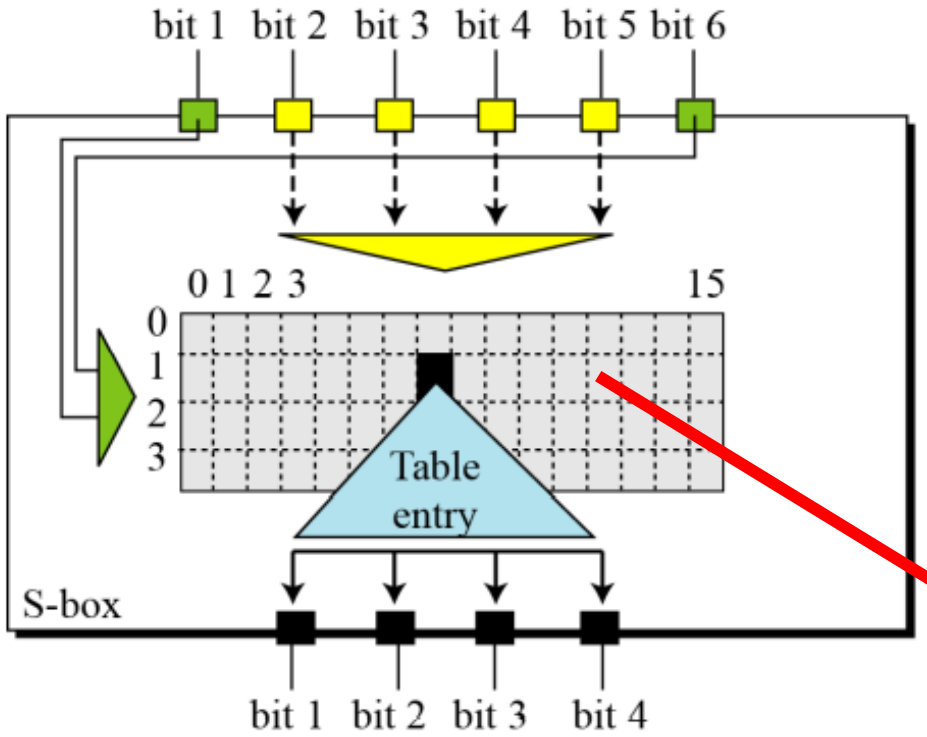



**Figure 6.7** ***S-boxes***

* There are 8 S-Boxes. Each one has its own table.

## Figure 6.8 *S-box rule*




* Each S-box has its own table.

## Table 6.3 *S-box 1*

| | *0* | *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* | *9* | *10* | *11* | *12* | *13* | *14* | *15* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *0* | 14 | 04 | 13 | 01 | 02 | 15 | 11 | 08 | 03 | 10 | 06 | 12 | 05 | 09 | 00 | 07 |
| *1* | 00 | 15 | 07 | 04 | 14 | 02 | 13 | 10 | 03 | 06 | 12 | 11 | 09 | 05 | 03 | 08 |
| *2* | 04 | 01 | 14 | 08 | 13 | 06 | 02 | 11 | 15 | 12 | 09 | 07 | 03 | 10 | 05 | 00 |
| *3* | 15 | 12 | 08 | 02 | 04 | 09 | 01 | 07 | 05 | 11 | 03 | 14 | 10 | 00 | 06 | 13 |

## *Key Generation*

***The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.***

Shifting

| Rounds | Shift |
|---|---|
| 1, 2, 9, 16 | one bit |
| Others | two bits |

**Table 6.12** *Parity-bit drop table*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 57 | 49 | 41 | 33 | 25 | 17 | 09 | 01 |
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 02 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 03 |
| 60 | 52 | 44 | 36 | 63 | 55 | 47 | 39 |
| 31 | 23 | 15 | 07 | 62 | 54 | 46 | 38 |
| 30 | 22 | 14 | 06 | 61 | 53 | 45 | 37 |
| 29 | 21 | 13 | 05 | 28 | 20 | 12 | 04 |

**Table 6.14** *Key-compression table*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 14 | 17 | 11 | 24 | 01 | 05 | 03 | 28 |
| 15 | 06 | 21 | 10 | 23 | 19 | 12 | 04 |
| 26 | 08 | 16 | 07 | 27 | 20 | 13 | 02 |
| 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 |
| 51 | 45 | 33 | 48 | 44 | 49 | 39 | 56 |
| 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |

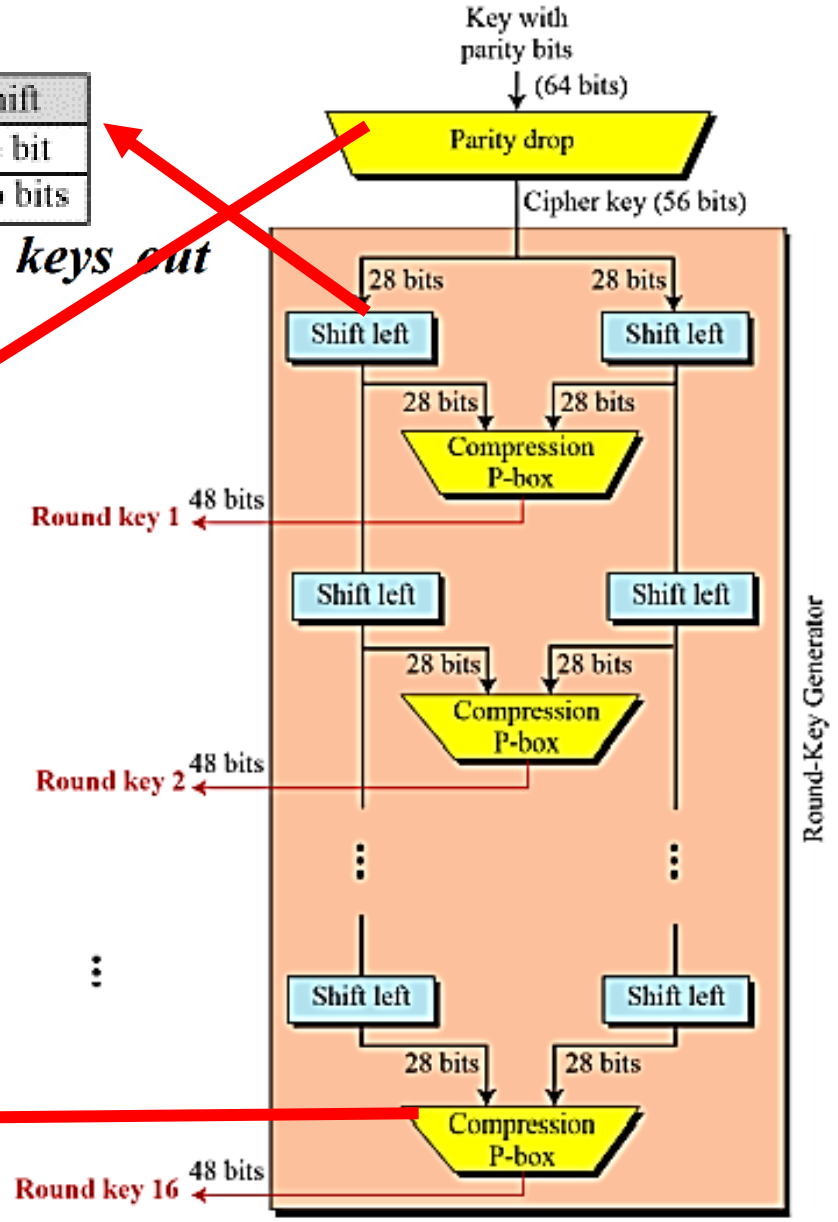



**Figure 6.10**
***Key generation***