B. Tech. III Year II semester

Computer Science and Engineering

CYBER SECURITY AND CYBER LAWS

Introduction to cyber Security, cryptography, Types of Attacks, Secrete Key Cryptography

Introduction: Cyber attacks, Defense Strategies and Techniques Mathematical background for Cryptography: Modulo arithmetic, The greatest common divisor, Useful Algebraic Structures, Chinese Remainder Theorem Basics of Cryptography: Secret versus Public key Cryptography, Types of attacks, Elementary substitution Ciphers, Elementary Transposition Ciphers, Other Cipher Properties Secrete Key Cryptography: Product Ciphers, DES Construction, Modes of Operation, MAC and other Applications, Attacks, Linear Crypt analysis.

Textbook

1. Network security and Cryptography by Bernard Menezes CENGAGE Learning Publications, 2010.

Introduction

- **Computer Security** is all about studying cyber attacks with a view to defending against them.
- **Cyber Attack** - an attempt by **hackers** to damage or destroy a computer network or system.
- **Motives** – "What are the main goals of an attacker"
  - Financial Gain
  - Recognition
  - Revenge/fun
  - Political motivation

Cyber Attacks include

- Company insiders
- Cyber terrorists – religious or political causes
- Theft of sensitive information- new products/military plans
- Political espionage – spying to get govt./national intelligence sensitive info.
- Disruption of service – unavailable/inaccessible
- Illegal access to or use of resources – free access/service (talk time, articles, journals, online products)

Other Definitions of Cyber Security

- Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
- The term cyber security refers to techniques and practices designed to protect digital data- stored, transmitted or used on an information system.

OR

Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks.

It is made up of two words one is cyber and other is security.

- Cyber is related to the technology which contains systems, network and programs or data.
- Whereas security related to the protection which includes systems security, network security and application and information security.

Why is cyber security important?

Listed below are the reasons why cyber security is so important in what's become a predominant digital world:

- Cyber attacks can be extremely expensive for businesses to endure.
- In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
- Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.
- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

Other Security domains and Cybersecurity

The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

Information security protects the integrity and privacy of data, both in storage and in transit.

Common Attacks

1. Attacks used to retrieve personal information from an individual.

- **Phishing attack** – through emails, SMS, weblinks
- **Pharming attack** - Pharming is a type of social engineering cyberattack in which criminals redirect internet users trying to reach a specific website to a different, fake site
- Pharming is much more effective than phishing because it doesn't require the user to click a link.

-- Continues

2. Attacks used for leakage of information

Skimming attack- Skimming is an act of copying the cardholder's personal payment information. Criminals employ different strategies for this purpose, such as photocopying receipts or more advanced methods, such as installing a small electronic device called a skimmer, mostly inside ATM or POS terminals, to store hundreds of victims' card numbers and PINs.

Side Channel attacks - An attack enabled by leakage of information from a physical cryptosystem

Eavesdropping or snooping – communication links

-- Continues

3. Intruding into a computer system

- Password guessing attacks – special case of dictionary attacks
- Identity theft – attacker is to impersonate the victim

4. Interruption/disruption of computing services

- Denial of Service(DoS) – making computing power, memory , bandwidth unavailable
- Slowing down web server
- Website defacement (modify the content of govt. website)

-- Continues

5. Malware

- **Virus** – It is a program that attempts to damage a computer system and replicates itself to other computer systems. It requires a host to replicate.
- **Worm**- A worm is a **self-replicating program** that can be designed to do any number of things, such as delete files or send documents via e-mail. A worm can negatively impact network traffic just in the process of replicating itself.

Viruses & worms use various spreading techniques like email, internet messages, webpages, Bluetooth and MMS

- **Trojan -** A Trojan horse is a malicious program that is disguised(masquerades) as legitimate software. The compromise of a user account could lead to the compromise of the entire environment. It cannot replicate.
- **Logic Bomb -** A Logic Bomb is malware that lies dormant until triggered. A logic bomb is a specific example of an asynchronous attack. A trigger activity may be a specific date and time, the launching of a specific program, or the processing of a specific type of activity. It does not self replicate.

-- Continues

- **Spyware –** installed on a machine, can be used to monitor user activity.
- **Keylogger –** used to observe key strokes, passwords
- **Ransomware -**a type of malicious software designed to block access to a computer system until a sum of money is paid.
- **Rootkit -** a set of software tools that enable an unauthorized user to gain control of a computer system without being detected.

If the elements are small, we call it "fine-grained," and if the elements are large, we call it "coarse-grained."

Vulnerabilities – is a weakness in a procedure, protocol, h/w or s/w in a organization, that has a potential to cause damage.

Human Vulnerabilities – induced by human behaviour.

Ex: user clicks on a link or email message (phishing attack, cross-site scripting attack)

Protocol Vulnerabilities – attacks on network protocols (TCP, IP, ARP etc.)

Ex: Attack on ARP protocol like to sniff passwords from the LAN. (Pharming Attack, hijacking attacks, man-in-the-middle- attack)

-- Continues

Software Vulnerabilities – related to application s/w

1. Executing malicious worm code in Program- Buffer overflow
2. Web server related – cross site scripting vulnerability
   - SQL injection vulnerability

Configuration Vulnerabilities – related to configuration settings on newly installed applications, files etc.

Ex: Privilege escalation attack

-- Continues

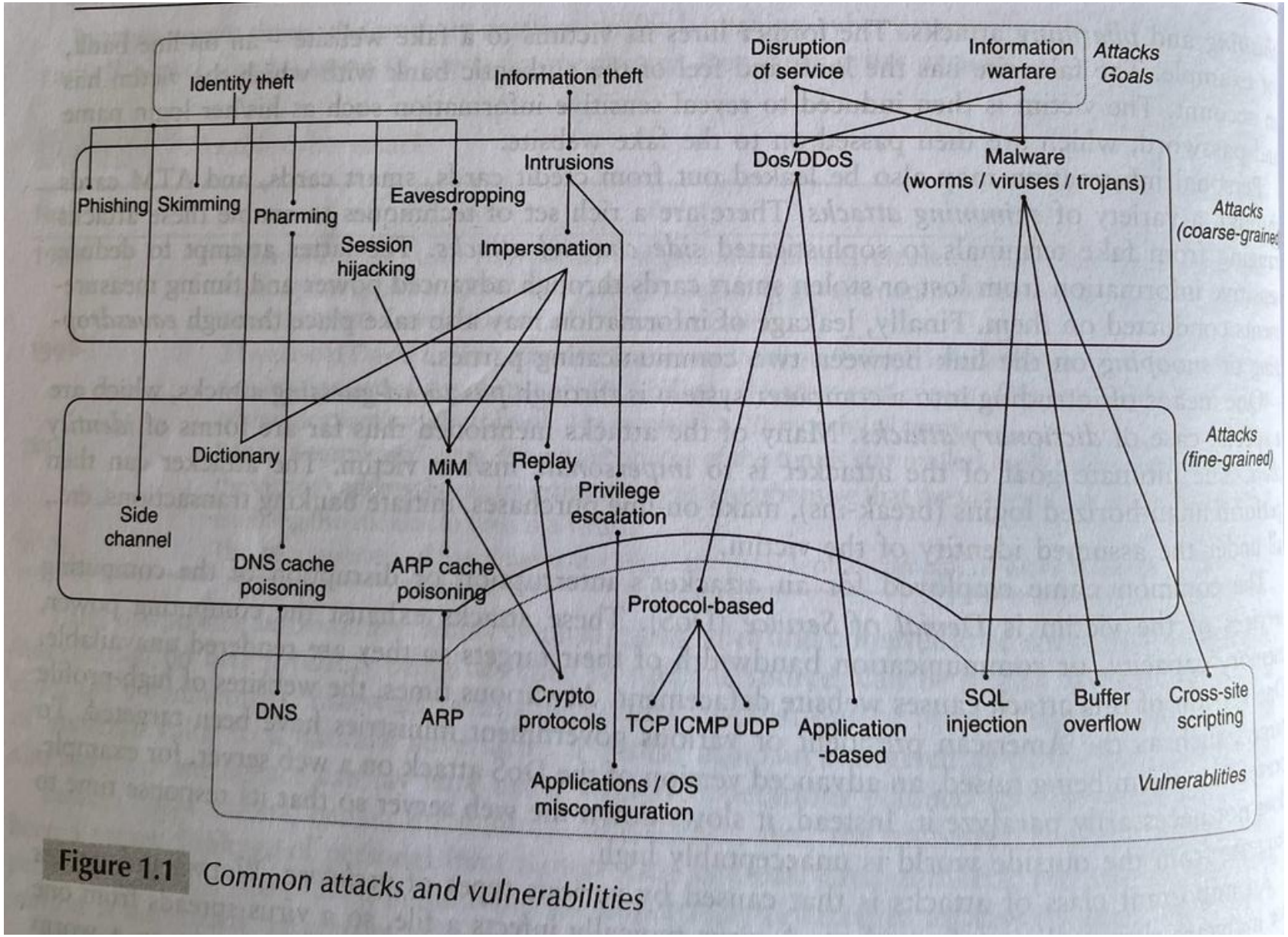


Figure 1.1 *Common attacks and vulnerabilities*

Defense Strategies and Techniques

1. Access Control – Authentication and Authorization
2. Data Protection
3. Prevention and Detection
4. Response, Recovery and Forensics

1. Access Control – Authentication and Authorization

Access control is a method of limiting access to a system or to physical or virtual resources

Access control systems perform identification, authentication, and authorization of users.

Authentication- Proof of identity

- password/pin
- biometric
- card/key

-- Continues

After successful authentication, the user may need several resources like files. Then system performs authorization.

Authorization is a process by which a server determines if the client has permission to use a resource or access a file.

2. Data Protection

Means assuring Data confidentiality, Data Integrity

-- cryptographic techniques used for encryption & decryption.

Methods – integrity check techniques, cryptographic checksum, symmetric/asymmetric

-- Continues

3. Prevention and Detection

-Access control and message encryption are preventive strategies.

-Code testing is used to detect vulnerabilities.

- black box testing, white box testing -- program

-intrusion preventive techniques – checks for worm signature or pattern or behaviour

-attack on packets – methods used are continuous monitoring, anomalous behaviour.

-- Continues

4. Response, Recovery and Forensics

Once the attack or infection has been detected, **response** measures need to be taken.

Like shutting down the system.

During worm detection, infected parts of system need to be quarantined, required patches must be applied.

Cyber forensics

Cyber forensics is a process of extracting data as proof for a crime

Mathematical background for Cryptography

Modulo Arithmetic

Let d be an integer and let n be a positive integer. Let q and r be the quotient and remainder obtained from dividing d by n. The relationship between d, n, q, and r is

$$d = n * q + r, 0 \leq r < n \quad \text{--(1)}$$

Note that r is a non-negative integer less than n. d and n are the dividend and the divisor, respectively. We say "d is equal to r modulo n" if the remainder obtained from dividing d by n is r. This is expressed as

$$r \equiv d \pmod{n} \qquad \text{--(2)}$$

For a given value of n and r, there are an infinite number of (d, q) pairs that satisfy Eq. 1.

Example: Let n = 10 and r = 3. Then 13, 23, 33, etc. all satisfy Eq. (1) with quotients 1, 2, 3, etc. In fact, each element of the set below satisfies Eq. (2).

.. -37, -27, -17, -7, 3, 13, 23, 33, 43, . . .}

-- Continues

Properties of modular arithmetic operations

- [(a mod n) + (b mod n)] mod n = (a + b) mod n
- [(a mod n) - (b mod n)] mod n = (a - b) mod n
- [(a mod n) x (b mod n)] mod n = (a x b) mod n

Where do we use these properties?

In cryptography, we often have to perform computations such as multiplying a large number of terms, each term itself being a very large number.

For example, we may have to multiply 50 integers, each about 1000 digits long.

-- Continues

★ System of arithmetic for integers.

★ Wrap around after reaching a certain value called modulus.

★ Central mathematical concept in cryptography.

-- Continues

Congruence

★ In cryptography, congruence(≡) instead of equality(=).

Examples:

$15 \equiv 3 \pmod{12}$

$23 \equiv 11 \pmod{12}$

$33 \equiv 3 \pmod{10}$

$10 \equiv -2 \pmod{12}$

$\therefore a \equiv b \pmod{m}$

i.e. $a = km + b$

$15 = 12 \times 1 + 3$

$23 = 12 \times 1 + 11$

$33 = 10 \times 3 + 3$

$10 = 12 \times 0 + 10$

$a = m \times k + b$

Ref: Modular Arithmetic (Part 1) - YouTube

The Greatest Common Divisor

The greatest common divisor (GCD) refers to the greatest positive integer that is a common divisor for a given set of positive integers.

- For a set of positive integers (a, b), the greatest common divisor is defined as the greatest positive number which is a common factor of both the positive integers (a, b). GCD of any two numbers is never negative or 0 as the least positive integer common to any two numbers is always 1. **If gcd(b,c) = 1, we say that b and c are relative prime or co-prime. An integer is prime if it is co-prime with all positive integers less than it.**
- There are two ways to determine the greatest common divisor of two numbers:
- By finding the common divisors
- By Euclid's algorithm

-- Continues

Euclid's Algorithm for Greatest Common Divisor

As per Euclid's algorithm for the greatest common divisor, the GCD of two positive integers (a, b) can be calculated as:

- If a = 0, then GCD (a, b) = b as GCD (0, b) = b.
- If b = 0, then GCD (a, b) = a as GCD (a, 0) = a.

If both a≠0 and b≠0, we write 'a' in quotient remainder form (a = b×q + r) where q is the quotient and r is the remainder, and a>b.

Find the GCD (b, r) as GCD (b, r) = GCD (a, b)

We repeat this process until we get the remainder as 0.

-- Continues

Example: Find the GCD of 12 and 10 using Euclid's Algorithm.

Solution: The GCD of 12 and 10 can be found using the below steps:
a = 12 and b = 10
a≠0 and b≠0
In quotient remainder form we can write 12 = 10 × 1 + 2
Thus, GCD (10, 2) is to be found, as GCD(12, 10) = GCD (10, 2)

Now, a = 10 and b = 2
a≠0 and b≠0
In quotient remainder form we can write 10 = 2 × 5 + 0
Thus, GCD (2,0) is to be found, as GCD(10, 2) = GCD (2, 0)

Now, a = 2 and b = 0
a≠0 and b=0
Thus, GCD (2,0) = 2

GCD (12, 10) = GCD (10, 2) = GCD (2, 0) = 2

Thus, GCD of 12 and 10 is 2.

Euclid's algorithm is very useful to find GCD of larger numbers, as in this we can easily break down numbers into smaller numbers to find the greatest common divisor.

Useful Algebraic Structures

Groups, rings, and fields are the important elements of a branch of mathematics called as abstract algebra, or modern algebra.

Group

- A group (G) is indicated by {G, *}. It is a group of elements with a binary operation ' * ' that satisfies four properties. The properties of Group are as follows –
- **Closure** – If a and b are elements of G, therefore c = a * b is also an element of set G. This can define that the result of using the operations on any two elements in the set is another element in the set.

REF: https://www.youtube.com/watch?v=vfyUU_prh9s

-- Continues

- **Associativity** – If a, b, and c are element of G, therefore

(a * b) * c = a * (b * c), means it does not substance in which order it can use the operations on higher than two elements.

- **Identity** – For all a in G, there occur an element e in G including I * a = a * I = a.
- **Inverse** – For each a in G, there occur an element a' known as the inverse of a such that a * a' = a' * a = e.
- A group is an abelian group if it satisfies the following four properties more one additional property of commutativity.
- **Commutativity** – For all a and b in G, we have a * b = b * a.

-- Continues

- **Ring** – A ring R is indicated by {R, +, x}. It is a set of elements with two binary operations, known as addition and multiplication including for all a, b, c in R the following axioms are kept –
- R is an abelian group regarding addition that is R satisfies properties A1 through A5. In the method of additive group, it indicates the identity element as 0 and the inverse of a as – a.
- **(M1): Closure under multiplication** – If a and b belong to R, then ab is also in R.
- **(M2): Associativity of Multiplication** – a(bc)=(ab)c for all a, b, c in R.
- **(M3): Distributive Laws** –
- a(b+c)=ab + ac for all a, b, c in R
- (a+b)c=ac+bc for all a, b, c in R

-- Continues

- **(M4): Commutative of Multiplication** – ab=ba for all a, b in R.
- **(M5): Multiplicative identity** – There is an element 1 in R including a1=1a for all a in R.
- **(M6): No zero divisors** – If a, b in R and ab = 0, therefore a = 0 or b = 0.
- **Field** – A field F is indicated by {F, +, x}. It is a set of elements with two binary operations known as addition and multiplication, including for all a, b, c in F the following axioms are kept –
- F1 is an integer domain that is F satisfies axioms A1 through A5 and M1 through M6.
- **(M7): Multiplication inverse** – For each a in F, except 0, there is an element a^{-1} in F such that $aa^{-1} = (a^{-1})a=1$.

Algorithm for Chinese Remainder Theorem

- **Step 1:-** Find $\mathbf{M} = m_1 \times m_2 \times \ldots \times m_k$. This is the common modulus.
- **Step 2:-** Find $\mathbf{M_1} = M/m_1$, $\mathbf{M_2} = M/m_2$, …,$\mathbf{M_k} = M/m_k$.
- **Step 3:-** Find the multiplicative inverse of M_1, M_2, …,M_k using the corresponding moduli (m_1, m_2, …, m_k). Call the inverses as:-

$$\mathbf{M_1^{-1}, M_2^{-1}, \ldots, M_k^{-1}}$$

- **Step 4:-**The solution to the simultaneous equations is:-

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M$$

Ref : The Chinese Remainder Theorem (Solved Example 1) – YouTube

2. Chinese remainder theorem and its applications (csusb.edu)

Basics of Cryptography

Recollect the terms

-cryptography

-provide message –confidentiality, integrity, authentication and digital signatures

-plaintext, ciphertext, encryption, decryption, encryption key, decryption key, encryption function

-Kerckhoff’s Pinciple – The secrecy should be in the key used for decryption not in encryption or decryption algorithm.

• Secret versus Public key Cryptography

Key	**It uses a single shared key (secret key) to encrypt and decrypt the message.**	**It uses two different keys for encryption and decryption.**
Size	**The size of ciphertext in symmetric encryption could be the same or smaller than the plain text.**	**The size of ciphertext in asymmetric encryption could be the same or larger than the plain text.**
Efficiency	**It is efficient as this technique is recommended for large amounts of text.**	**It is inefficient as this technique is used only for short messages.**
Speed	**The encryption process of symmetric encryption is faster as it uses a single key for encryption and decryption.**	**The encryption process in asymmetric encryption is slower as it uses two different keys; both keys are related to each other through the complicated mathematical process.**
Purpose	**Symmetric encryption is mainly used to transmit bulk data.**	**It is mainly used in smaller transactions. It is used for establishing a secure connection channel before transferring the actual data.**
Security	**It is less secured as there is a use of a single key for encryption.**	**It is safer as there are two keys used for encryption and decryption.**
Algorithms	**The algorithms used in symmetric encryption are 3DES, AES, DES, and RC4.**	**RSA, DSA, Diffie-Hellman, ECC, Gamal,**

Types of Attacks

Cryptographic algorithm is secure if a cryptanalyst is unable to

a) Obtain the corresponding plaintext from a given ciphertext
b) Deduce the secret key or private key

-Known cipher text

-known plaintext

-chosen plaintext

-brute force attack

Elementary substitution Ciphers

1. Caeser cipher – each letter is substituted for another unique letter
2. Monoalphabetic Ciphers -The “cipher” line can be any permutation of the 26 alphabetic characters. This would seem to eliminate brute-force techniques for cryptanalysis. A single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message. English language - Nature of plain text is known.
3. Polyalphabetic cipher – the cipher text correspond to a particular character in the plaintext is not fixed.

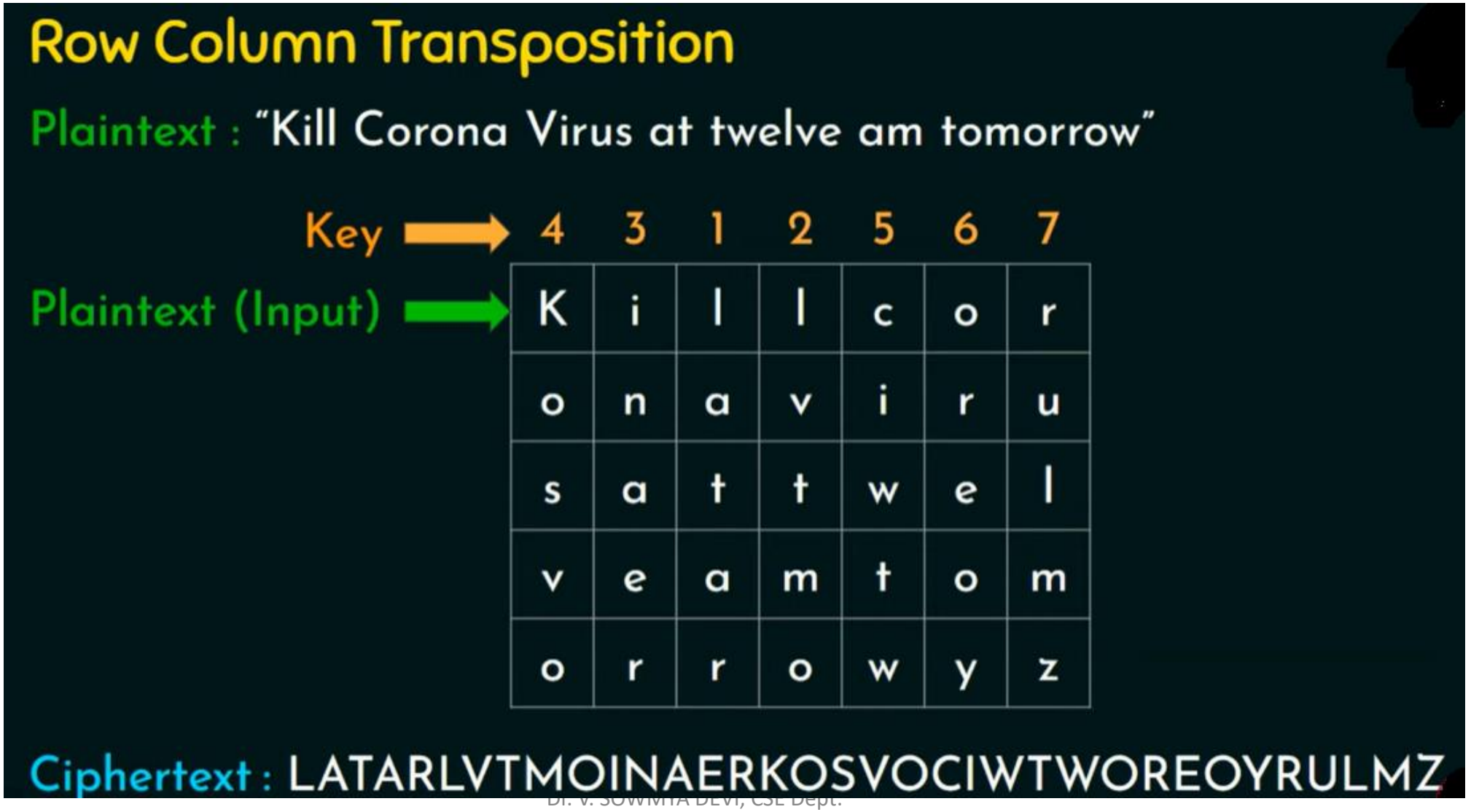
- Vigenere Cipher
- The Hill Cipher

Ref - Vigenere Cipher – javatpoint

Hill Cipher (Encryption) - YouTube

Elementary Transposition Ciphers

-means shuffling, rearranges or permutes the bits in a block of plain text.



2. Block Ciphers and stream ciphers

Parameters	Block Cipher	Stream Cipher
Definition	Block Cipher is the kind of encryption that converts plaintext by taking each block individually.	Stream cipher is the kind of encryption that converts plaintext by taking one byte of the plaintext at a time.
Principle	It uses both diffusion and confusion principles for the conversion (used later in encryption).	Only the confusion principle is used by Stream Cipher for the conversion.
Decryption	In Block cipher, *reverse encryption or decryption* is more difficult than stream cipher since more bits are combined to be encrypted in this scenario.	In a stream cipher, XOR is used for encryption that can quickly converted back to plain text.
Implementation	Feistel Cipher is the most popular block cipher implementation.	Vernam Cipher is the main implementation of Stream Cipher.
Reversibility	It is difficult to reverse encrypted text.	It uses XOR encryption, which is easily reversed to the plain text.
Algorithm modes used	ECB (Electronic Code Book) CBC (Cipher Block Chaining)	CFB (Cipher Feedback) OFB (Output Feedback)
Complexity	Simple design	Complex comparatively
No of bits used	64 Bits or more	8 Bits

Cipher Properties:

1. Confusion and diffusion

Confusion -the technique assures that the ciphertext has no information about the plaintext

diffusion -the output bits must be challengingly dependent on the input bits so that if the plaintext is modified by only one bit, the ciphertext must change in an many bits.

Key Cryptography: Product Ciphers

- Cipher which use permutation(P-box) and substitution (S-box) boxes

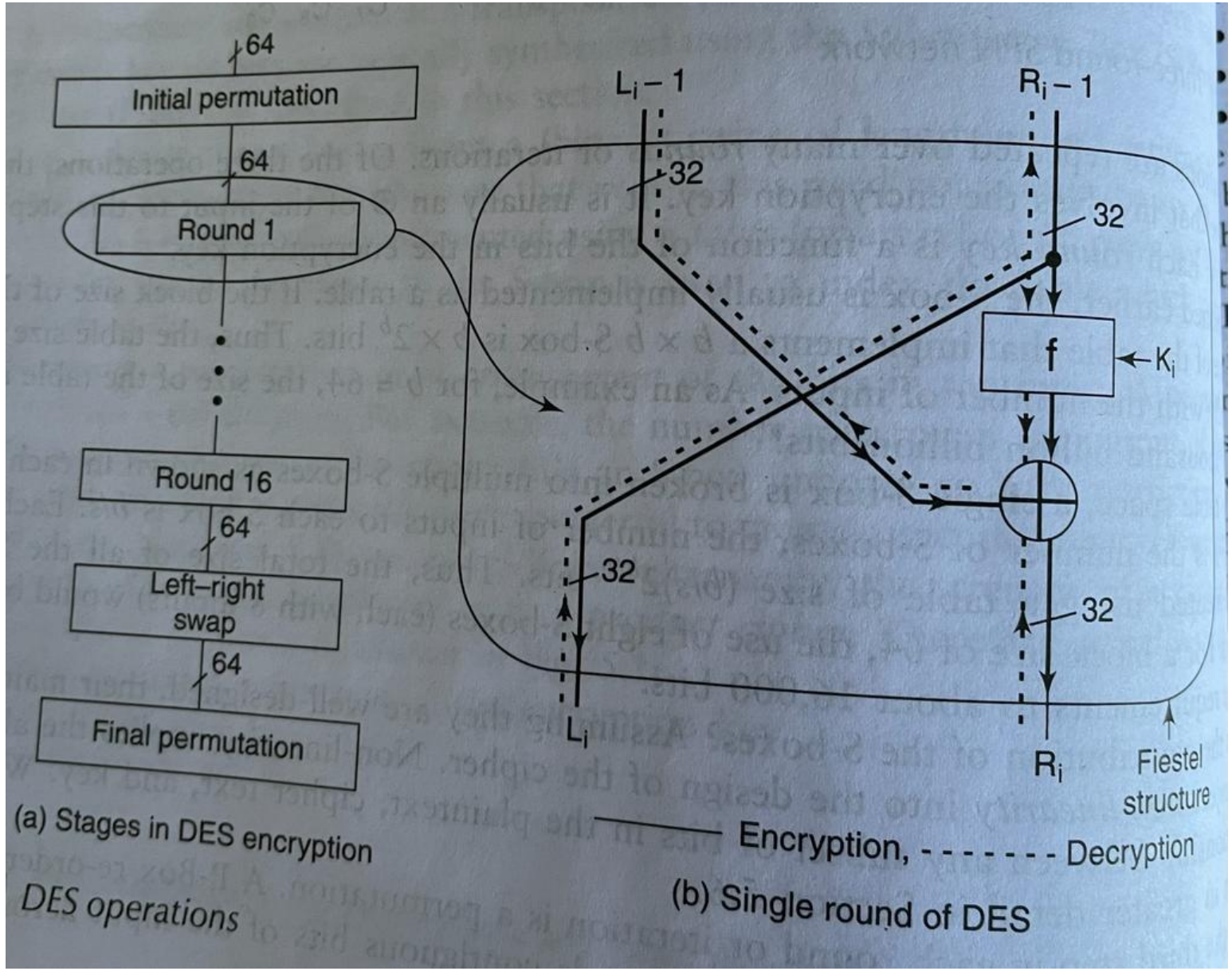
DES Construction: symmetric key

Fiestel structure:

- initial permutation
- 16 rounds of a given function
- a 32-bit left right swap
- a final permutation

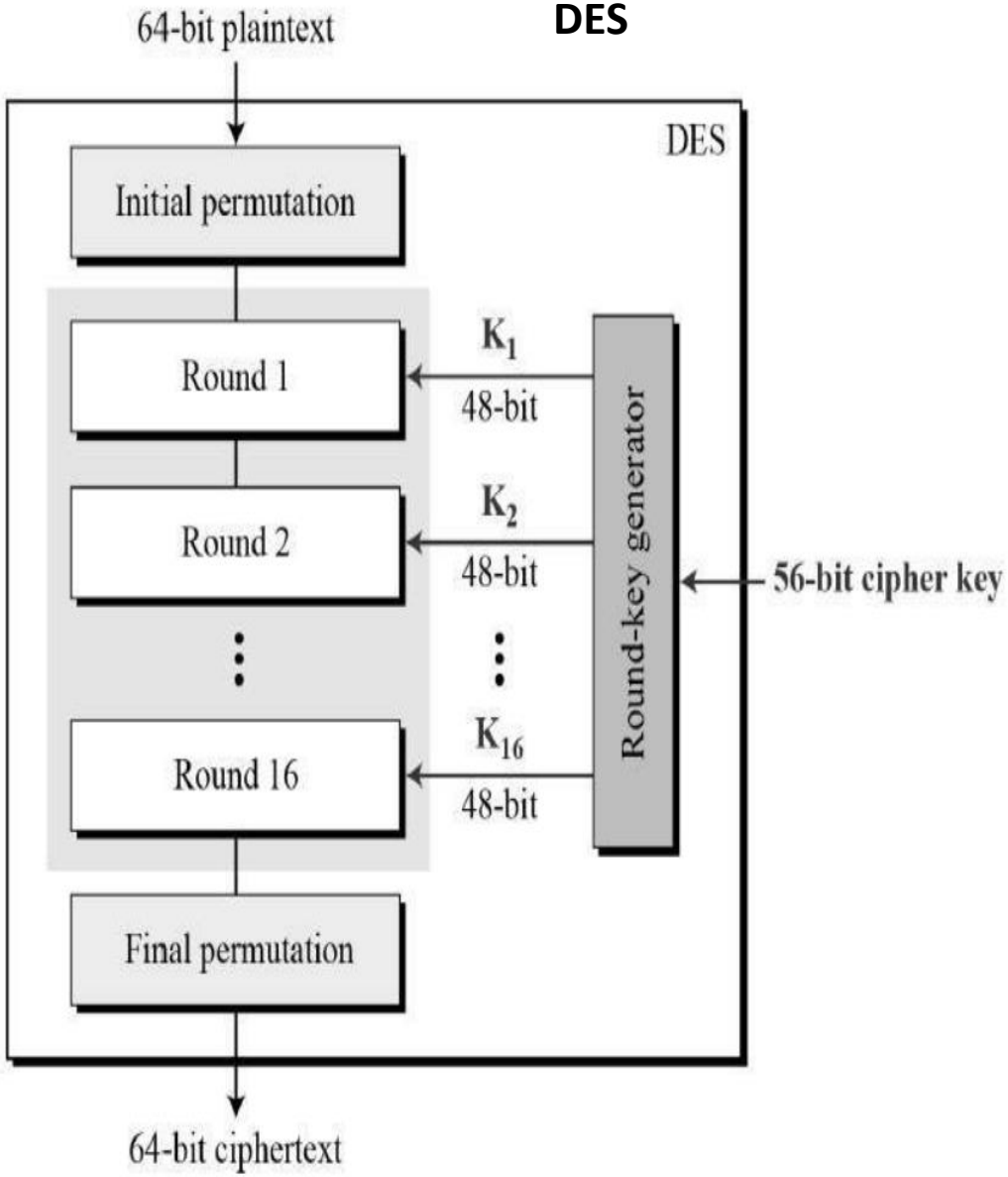
Round function

- Expansion
- XoR with a round Key
- Substitution
- Permutation



DES operations

DES



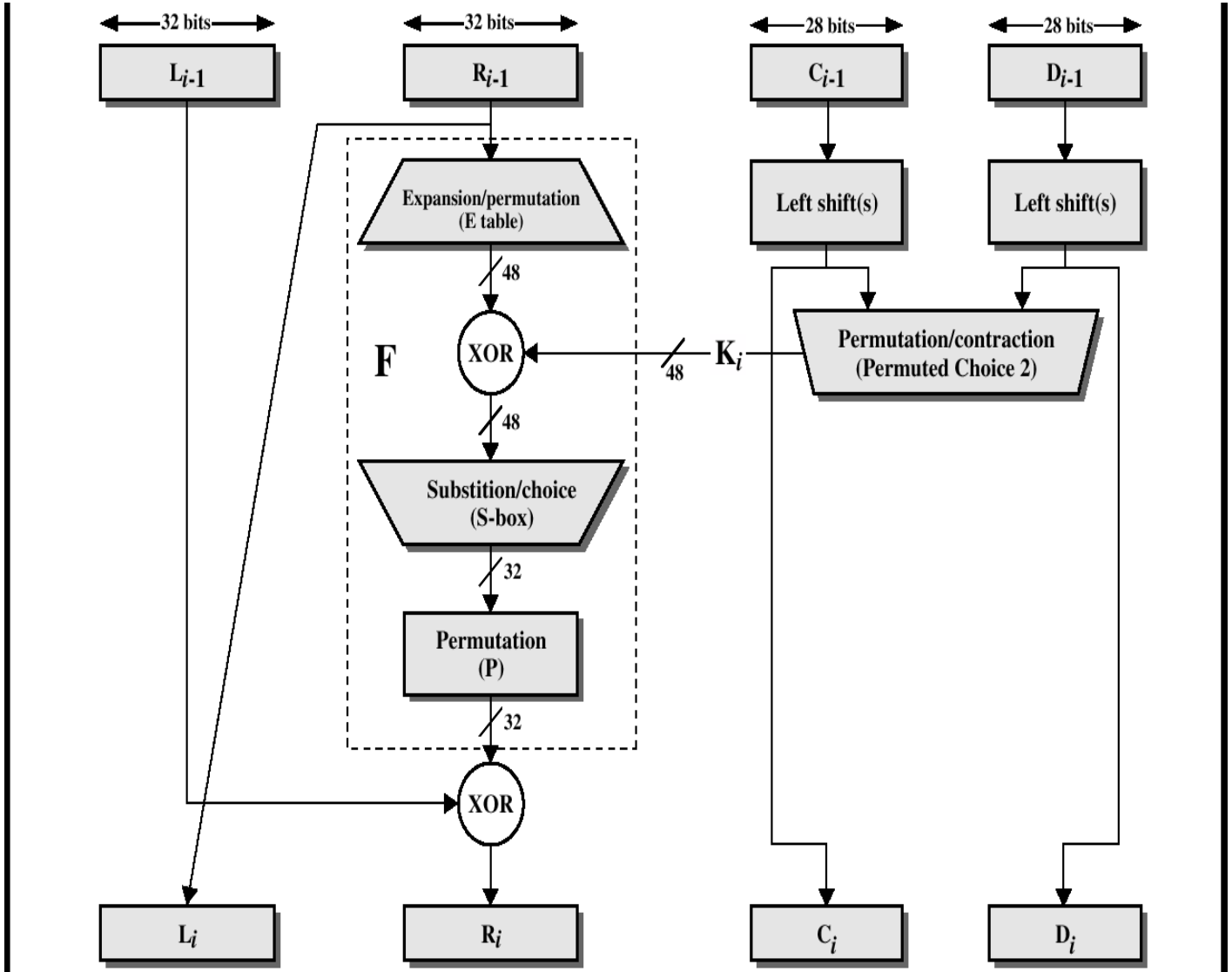


Figure 2.4 Single Round of DES Algorithm

DES Round Structure

- uses two 32-bit L & R halves
- as for any Feistel cipher can describe as:

  $L_i = R_{i-1}$

  $R_i = L_{i-1} \oplus \mathrm{F}(R_{i-1}, K_i)$
- F takes 32-bit R half and 48-bit subkey:
  - expands R to 48-bits using perm E
  - adds to subkey using XOR
  - passes through 8 S-boxes to get 32-bit result
  - finally permutes using 32-bit perm P

Modes of Operation

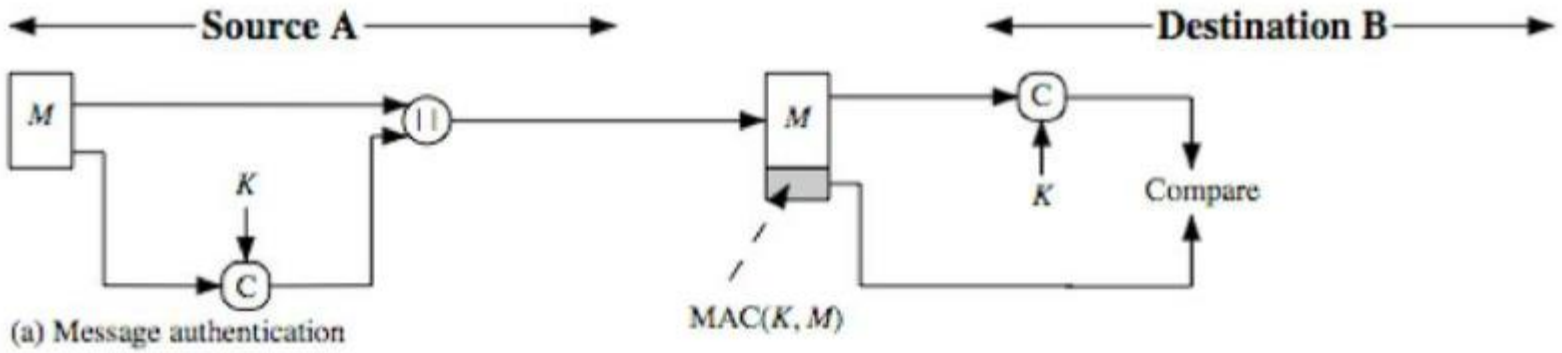
In 1980 the first four modes of operation was developed for DES (which also can be used with AES):

- The electronic codebook (ECB) mode
- The cipher block chaining (CBC) mode
- The cipher feedback (CFB) mode
- The output feedback (OFB) mode

Ref : Block cipher mode of operation - Wikipedia

Message Authentication Code:

- A function of the message and a secret key that produces a fixed-length value that serves as the authenticator
- Generated by an algorithm :
  - generated from message + secret key : **MAC = C(K,M)**
  - A small fixed-sized block of data
  - appended to message as a **signature** when sent
- Receiver performs same computation on message and checks it matches the MAC



Linear Crypt analysis

Linear cryptanalysis is a known plaintext attack, in which the attacker studies probabilistic linear relations referred to as linear approximations among parity bits of the plaintext, the Ciphertext and the hidden key.

Step1: Identifying Linear relationships

Step2: Using known Plaintext-Ciphertext pairs

Ref : Differential and Linear Cryptanalysis - GeeksforGeeks