Overview of Computer Security

Computer Security Concepts

Computer Security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

CIA Traid


CIA Triad
C
CONFIDENTIALITY
Confidentiality means the prevention of unauthorized disclosure of information.
01
I
INTEGRITY
Integrity means maintaining and assuring that data cannot be modified in an unauthorized or undetected manner.
02
A
AVAILABILITY
Availability means information should be readily accessible for the authorized users
03

- **Confidentiality:** Unauthorized access of the data should be restricted.
    - **Data Confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals. For example: Email Address, SSN, Personal contact numbers
    - **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. For example: Photos, videos, locations, family informations, Bank Account details etc

- **Integrity:** The data is not tampered in any way
    - **Data Integrity:** Assures that information and programs are changed only in a specified and authorized manner.
    - **System Integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability: Assures that the system works promptly and service is available and not denied to the authorized users. For example: Whenever the authorized users want to access the data, the data should be available to them.

Computer Security

- Computer security is the act of protection of computer systems and keep critical information from unauthorized access, theft or misuse.
- Hardware is secured the same way as any sensitive equipments, but system access and authorization are protected through various protocol.
- This includes Admin restriction to normal users, external devices such as pendrives, flash drives should be disabled by the admin

Information Security

- It is the act of protecting the information by mitigating the informations risks.
- It involves the protection of information system, information processed, stored and transmitted by the system from unauthorized access, use, disruption, modification and destruction

Network Security

- Act of protecting your network and data from different kind of breaches, intrusion and other threats
- It involves access control, virus and anti virus software, application security, network analytics , firewall, VPN, encryption and more

Threats

- It is a possible security violation that might exploit the vulnerability of a system or assets
- It may or maynot be malicious
- Can be initiated by the system itself as well as outsider
- Comparatively hard to detect

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

Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure 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. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **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. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception 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. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption 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. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation 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. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

Source: Based on RFC 4949

Attack

- It is deliberate unauthorized action on a system of assets
- It is intentional and malicious
- Types:
  - Active attack: It involves some modifications of the data stream or the creation of a false stream.
  - Passive attack: Just monitoring of the data transmission to find any leaks or informations

Assets

- Assets can be categorized as hardware, software, data and communication lines and network
- Anything that is useful and important to the organization can be classified as an assets. For example: hardware like CD-ROM, some private software, data, network lines etc

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 CD-ROM or DVD 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.

Security Requirements

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Incident Response
- Physical and Environmental Protection
- Personnel Security
- Risk Assessments
- System and Acquisitions
- System and Information Integrity

Attack Surface

- An attack surface consist of the reachable and exploitable vulnerabilities in a system.
    - Open ports on outward facing Web and other servers, services running on these ports
    - Services available on the inside of the firewall
    - Interfaces, SQL and Web forms
    - Code that processes the incoming data, email, XML, office documents and industry specific custom data exchange format
    - An employee with access to sensitive information vulnerable to social engineering attack

Types of Attack Surfaces

Network attack surface: This category refers to vulnerabilities over an enterprise network, WAN or the Internet.

- DOS and DDoS
- Disruption of communications links
- Various forms of intruder attack such as Man in the Middle attack, tapping etc

Types of Attack Surfaces

- **Software attack surface:** This refers to the vulnerabilities in application, utility, or operating system code.
  - Web Servers
  - Softwares with outdated components

Types of Attack Surfaces

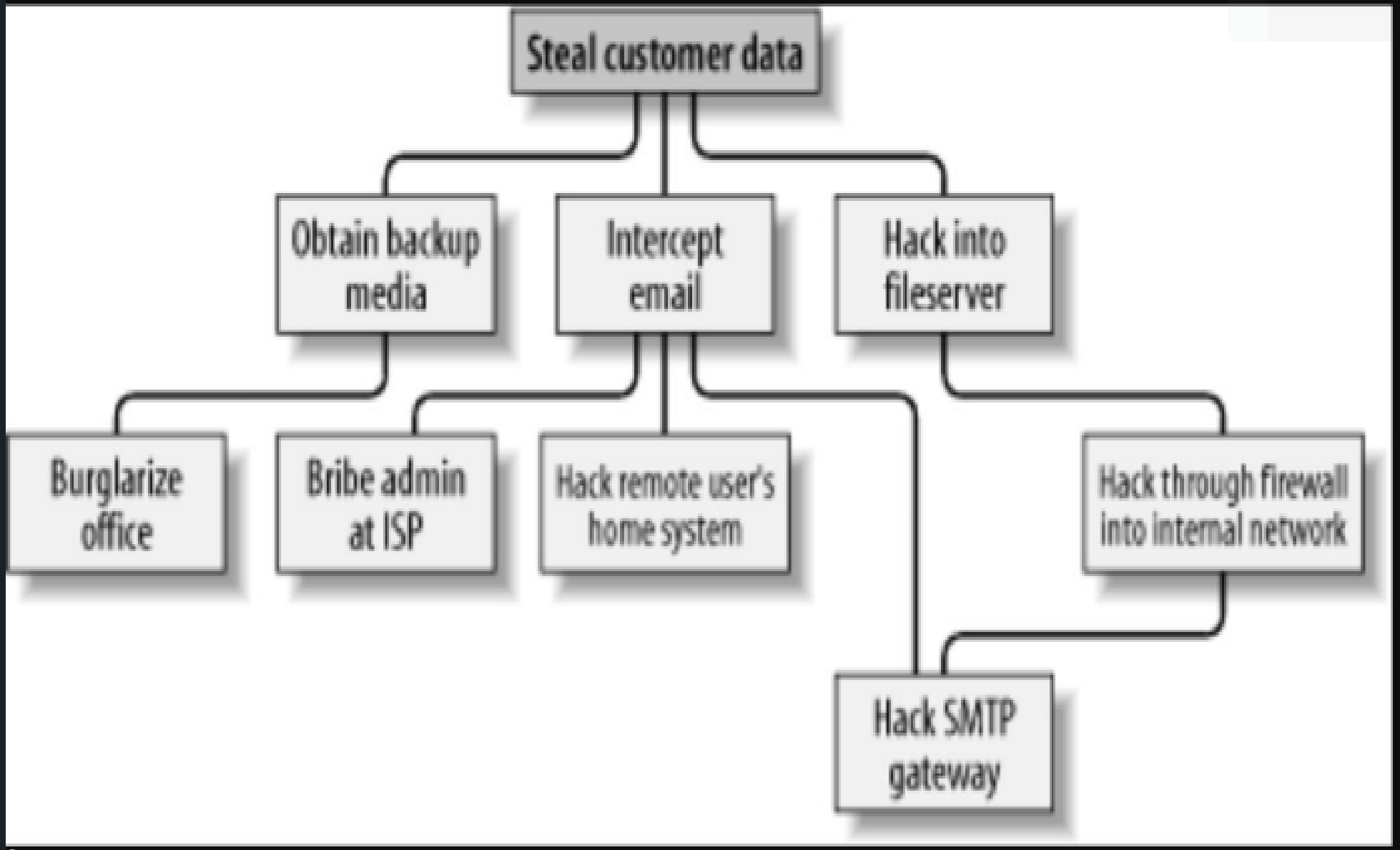
- **Human attack surface:** This category refers to vulnerabilities created by personnel or outsiders, such as social engineering, human error and trusted insiders

Attack Tree

- An attack tree is a multi-level diagram that describes threats on computer system and how a cyberattack can realize those threats.
- An attack tree can be huge and complex at times which can even contains thousands of different paths that can lead to cyber attack
- The attack trees are useful in determining what threats exists on computer system and how to mitigate these threats

Architecture of Attack Tree

1. Starts at the bottom (leaf node)
2. Advance to parents node by making child nodes, conditionals true (AND, OR)
3. The Attack is successful is it reached to top, else repeat STEP 2



Computer Security Strategy

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

Computer Security Strategy

Security Policy: Factors needs to be consider while developing security policy

- The value of assets being protected
- The vulnerabilities of system
- Potential Threat and likelihoods of attacks
- Ease of use VS Security
- Cost of security VS cost of failure and recovery

Computer Security Strategy

Security Implementation:

- Prevention:
- Detection:
- Response:
- Recovery

Computer Security Strategy

Assurance and Evaluation:

- Does the security system design meets its requirements ?
- Does the security system implementation meets its requirements ?

Evaluation: It is the process of examining computer system of products with respect to certain criteria. It involves testing and may also involve formal analytics or mathematical techniques.

CHAPTER 2

Cryptographic Algorithm

Classical Cryptosystems

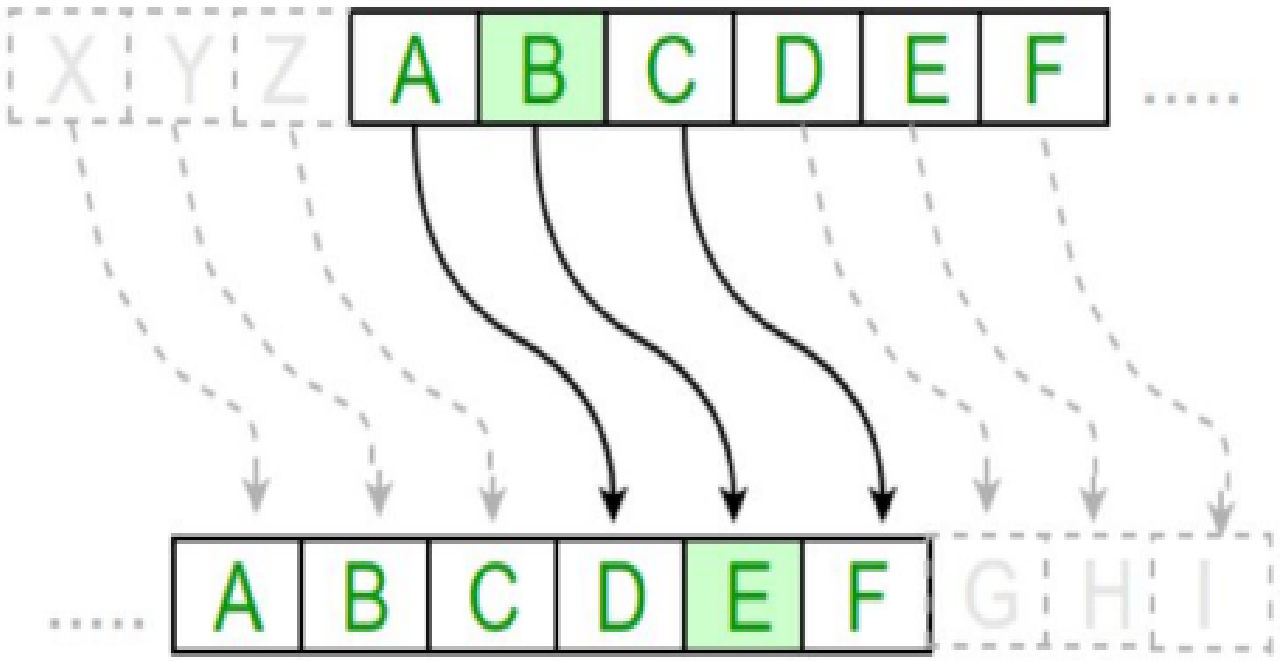
- **Caesar:** It is simply type of substitution system, i.e. each letter of a given text is replaced by a letter with a fixed number of position of the alphabet. For example: With a shift of 1, A -> B -> C etc

$$E_n(x) = (x + n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

(Decryption Phase with shift n)



Examples:

```
Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Shift: 23
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Text : ATTACKATONCE
Shift: 4
Cipher: EXXEGOEXSRGI
```

Caesar Cipher

Advantages:

- Easy to implement
- Requires only small pre-shared information
- Can be modified easily to make more secure, like using multiple shifts

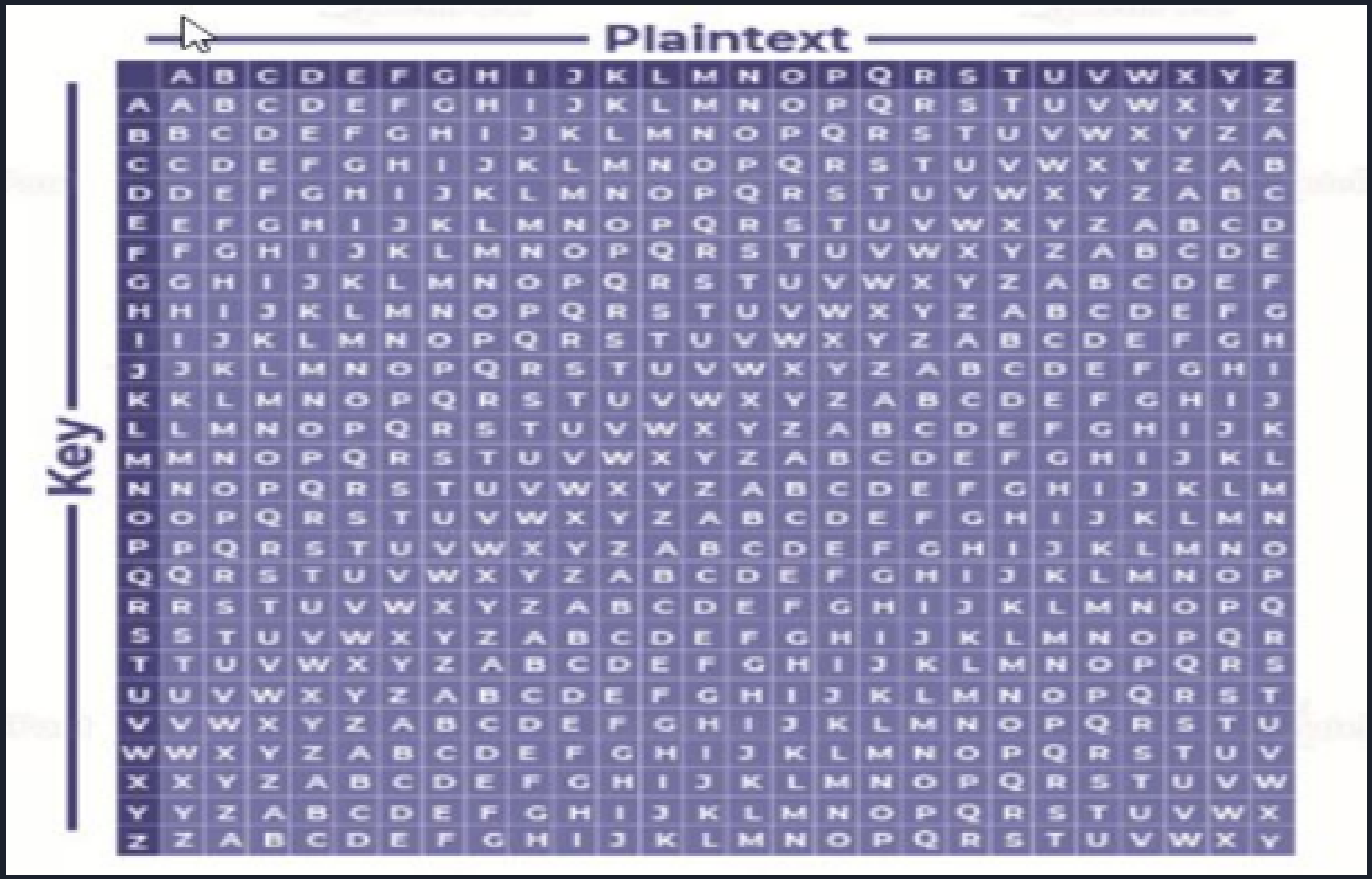
Disadvantages:

- It is not secure against modern decryption methods
- Doesn't provide confidentiality, integrity, and authenticity in a message
- Not useful for long messages as it can be cracked more easily

Classical Cryptosystems

Vigenere: It is a polyalphabetic substitution cipher, which means that the cipher alphabet is changed regularly during the encryption process, due to this, the cipher become less vulnerable to cryptanalysis

Vigenere Cipher Table



Vigenere Cipher method

Encoding Method:

- Get your plain text and key
- Level both the plain text and key via repeating the key
- Use the vigenere table to find the corresponding value

Decoding Method:

- Get your cipher value and key
- Level both cipher and key via repeating the key
- Use the vigenere table to decode and get the original text

Classical Cryptosystems

Playfire Cipher: A pair of alphabets are encrypted instead of one at a time

- Generate a 5*5 matrix , usually ignoring the j in the matrix
- If a plain text contains j , it is replaced by i
- Initial alphabets in the matrix is key then the remaining words of the alphabets

Playfair cipher Algorithm

1. The plain text is split into pairs of two letters, if there is odd letter , Z is added to last letter
2. Pair cannot be made with same letter, break the letter and add bogus letter x
3. If the letter is standing alone in the process of pairing, then add extra bogus letter with alone letter

Rules of Encryption:

- If both the letter are in same column, take the letter below each
- If both the letter are in same row, take the letter to the right
- If neither of the rule is true, form a rectangle and take letter on the horizontal opposite corners of rectangle

Classical cryptosystems

Rail Fence cipher: The plain text is written down as a sequence of diagonals and then read off as sequence of rows depending on the depth given

Encryption: write the plain text as per the depth down the sequence of the diagonal and read off as sequence of rows

Decryption:

1. make a table with no.of words as column and rows as depth
2. Fill the first rows from the encrypted text to first row
3. Fill the remaining words to the down the rows and continue this process till all the words are covered
4. Read the sequence as rows which gives us the plain text

Modern Ciphers

Block Vs Stream Ciphers

Stream Cipher:

- It is the one that encrypts the digital data stream one bit or 1 bit at a time.
- It is a symmetric key cipher (one key for both encryption and decryption)

Steam Cipher mechanism

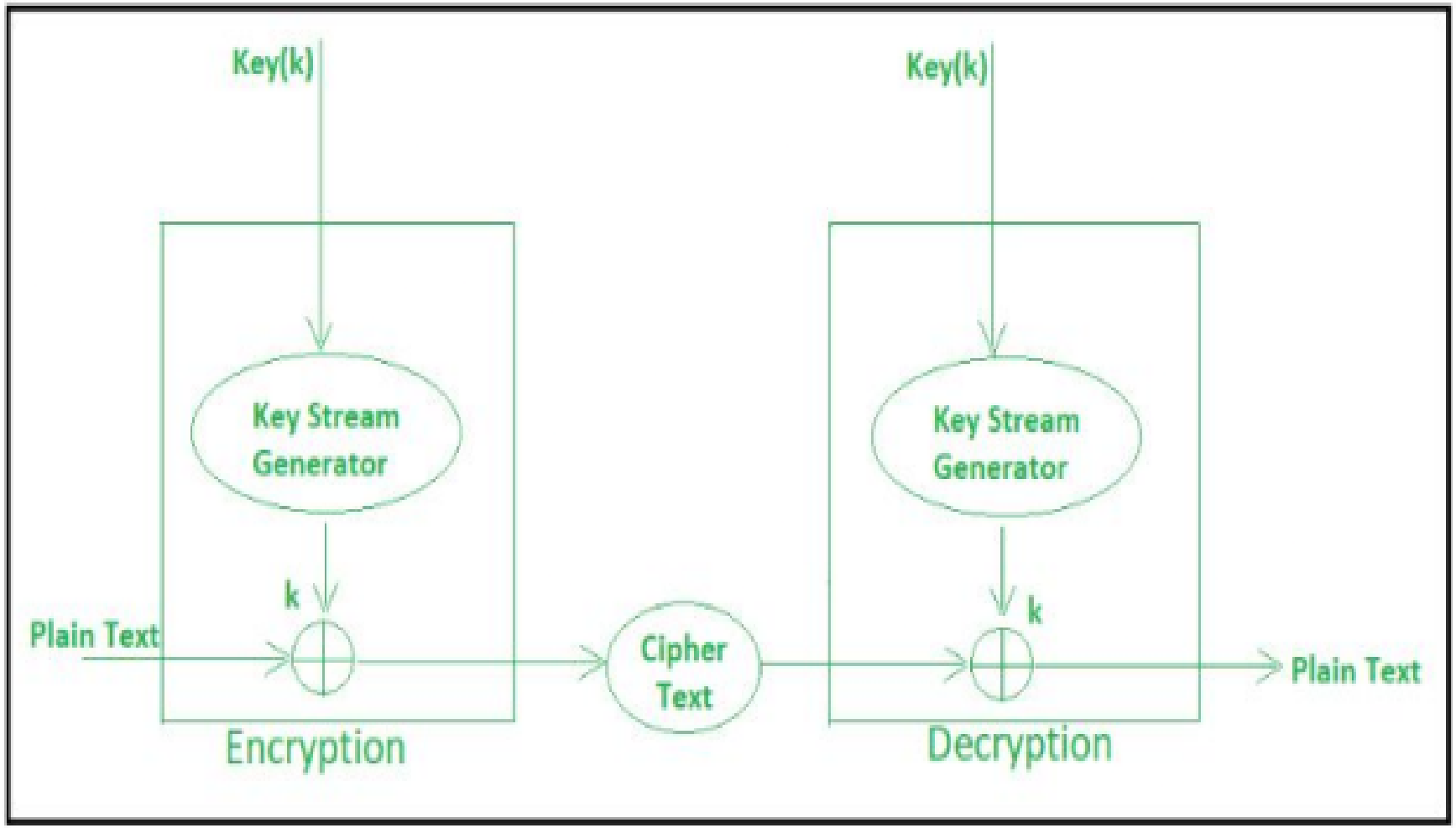


Diagram of Stream Cipher

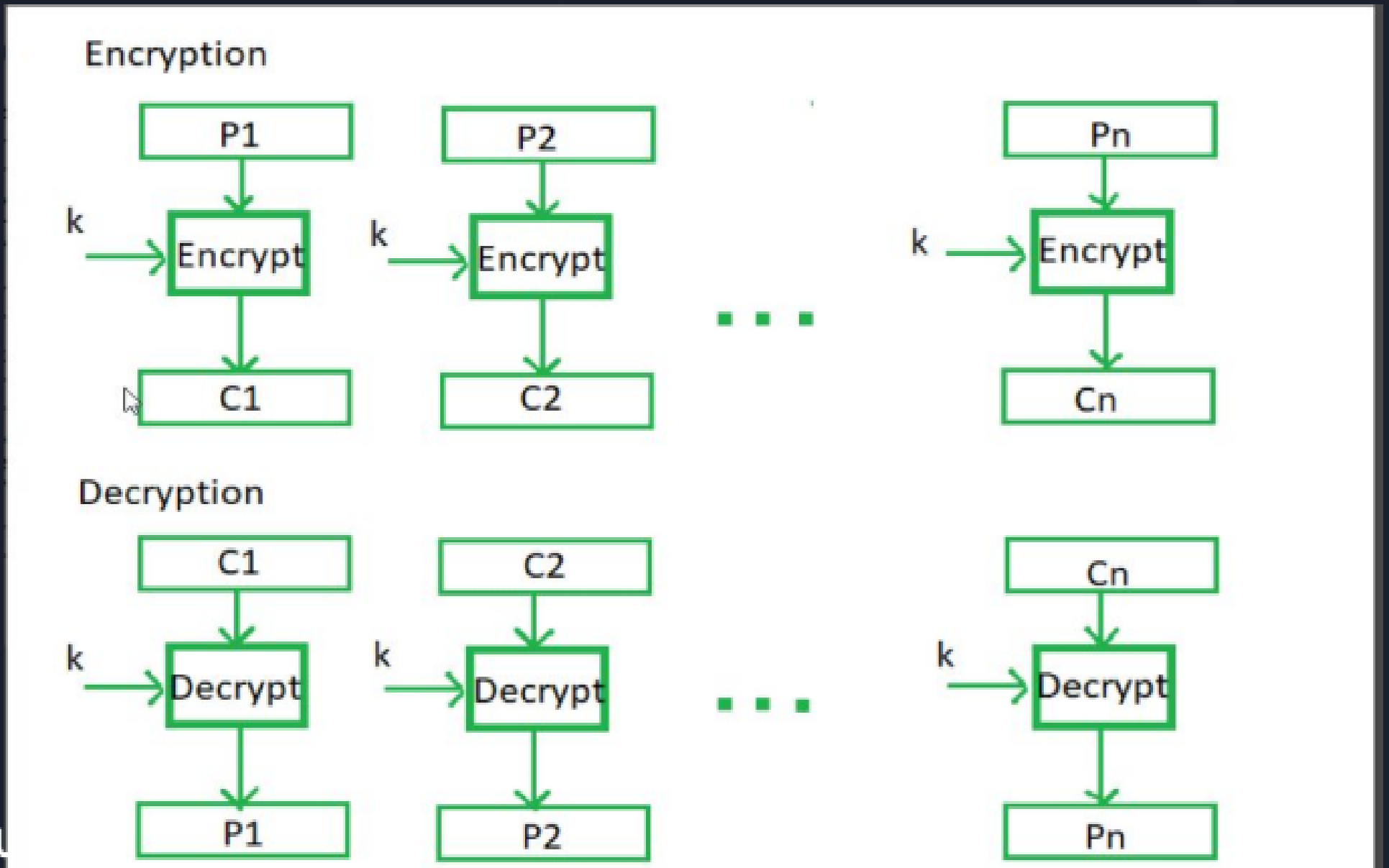
Modern Ciphers

Block Cipher: It is an encryption algorithm that takes a fixed size of input say x bits and produce a cipher text of x bits again.

Modes of Block Cipher:

- Electronic Code Book (ECB): It is the easiest block cipher mode of functioning.It is easier because of direct encryption of each block of input plain text and output is in form of encrypted ciphertext

Electronic Code Block (ECB)



Electronic Code Block (ECB)

Advantages:

- Parallel encryption of blocks of bits is possible, thus faster way of encryption.
- Simple way of block cipher

Disadvantages:

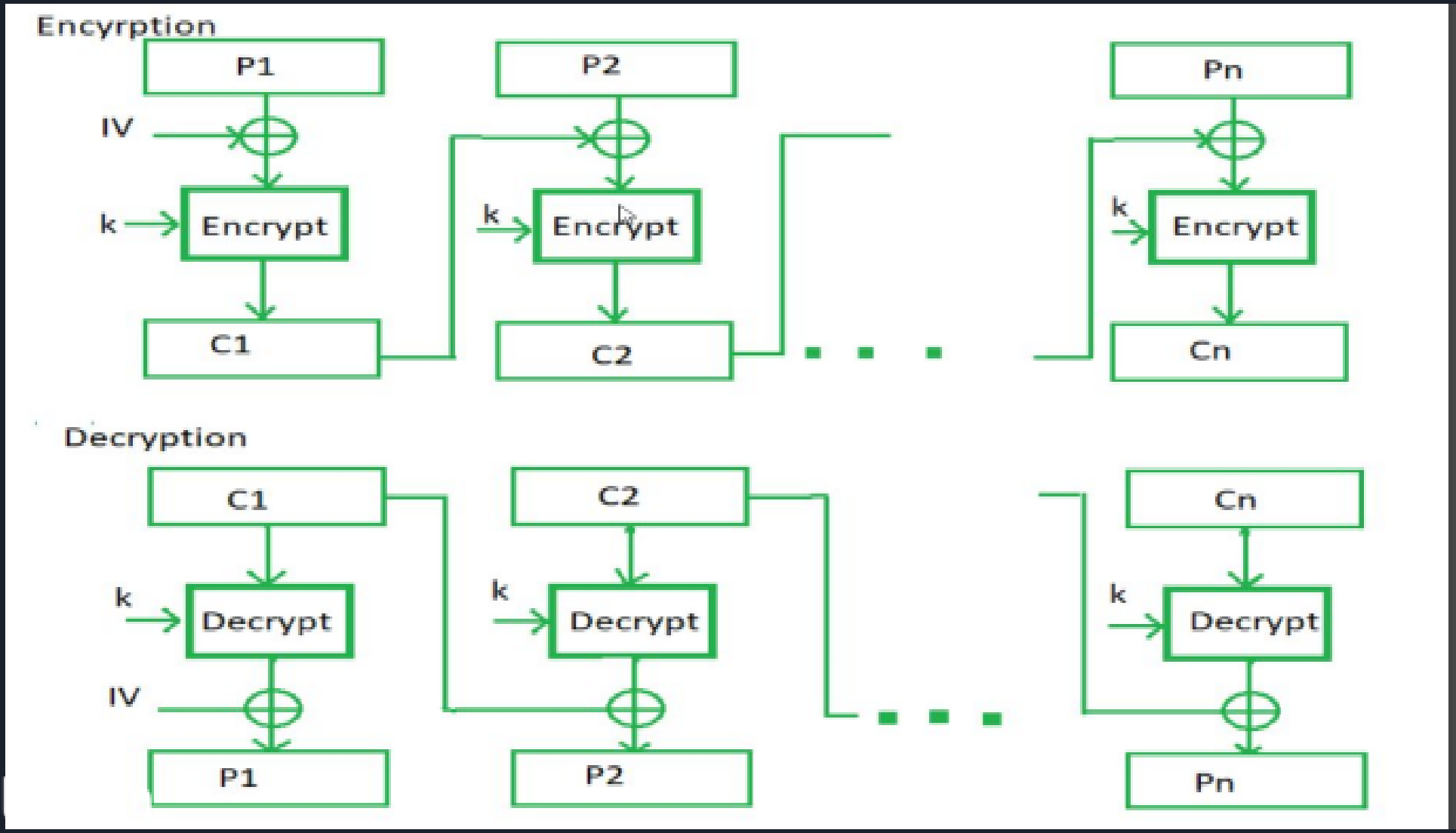
- Prone to cryptanalysis since there is direct relationship between ciphertext and plain text

Cipher Block Chaining (CBC)

It is the advancement of ECB. In CBC , the previous cipher block is given as input to the next encryption algorithm after XOR with original plaintext block.

- A Cipher block is produced by encrypting an XOR output of the previous cipher block and present plaintext block

Cipher Block Chaining



Cipher Block chaining (CBC)

Advantages:

- CBC works well for input greater than b bits
- It is good authentication mechanism
- More secure than EBC

Disadvantages:

- Parallel encryption is not possible since every encryption requires a previous cipher

Block Ciphers

Other modes:

- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFB)
- Counter Mode

S.NO	Block Cipher	Stream Cipher
1.	Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.	Stream Cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.
2.	Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
3.	The complexity of block cipher is simple.	While stream cipher is more complex.
4.	Block cipher Uses confusion as well as diffusion.	While stream cipher uses only confusion.
5.	In block cipher, reverse encrypted text is hard.	While in-stream cipher, reverse encrypted text is easy.
6.	The algorithm modes which are used in block cipher are ECB (Electronic Code Book) and CBC (Cipher Block Chaining).	The algorithm modes which are used in stream cipher are CFB (Cipher Feedback) and OFB (Output Feedback).
7.	Block cipher works on transposition techniques like rail-fence technique, columnar transposition technique, etc.	While stream cipher works on substitution techniques like Caesar cipher, polygram substitution cipher, etc.
8.	Block cipher is slow as compared to a stream cipher.	While stream cipher is fast in comparison to block cipher.

Modern Ciphers

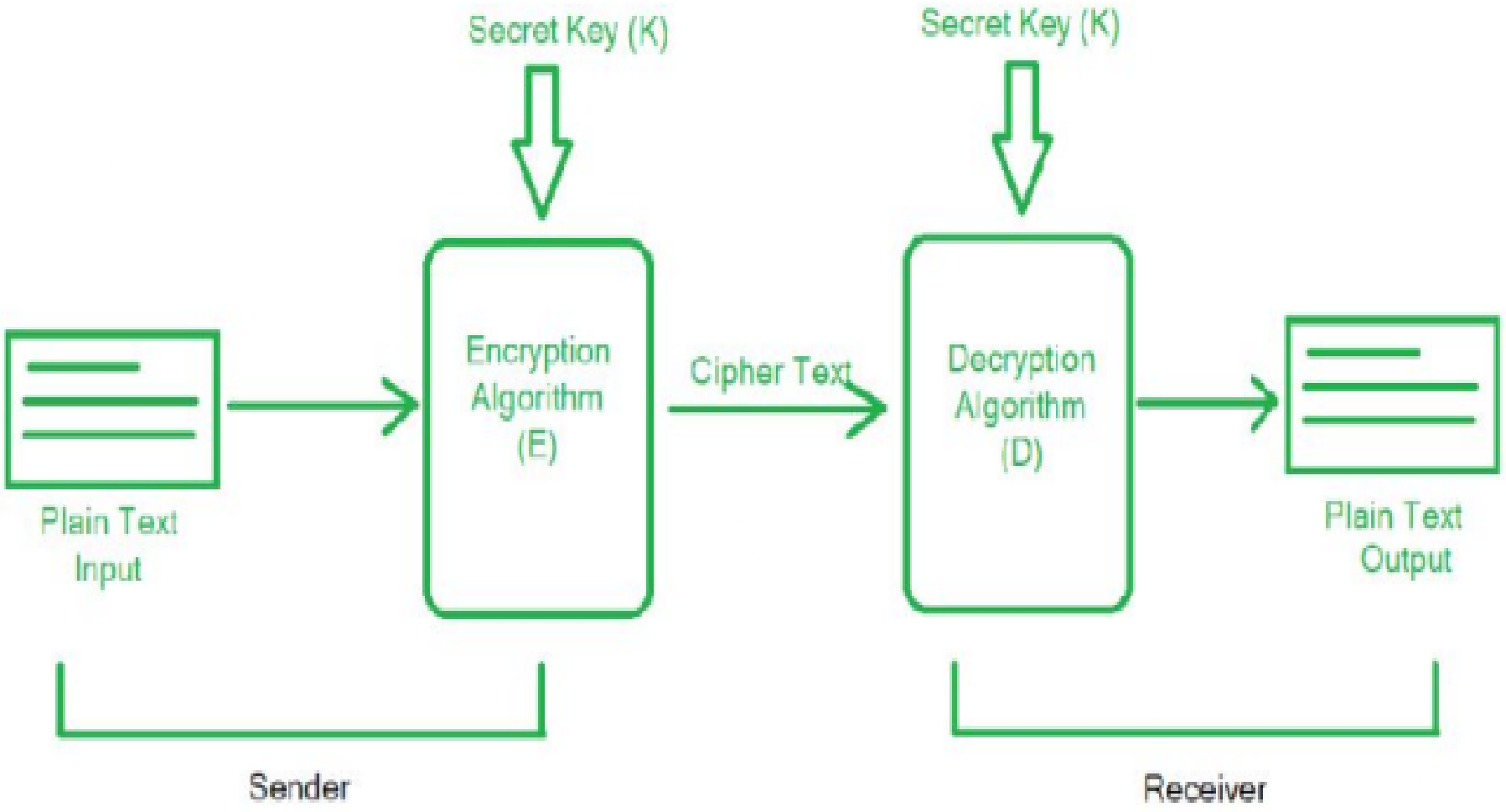
Symmetric Vs Asymmetric Ciphers

Symmetric Ciphers:

- It uses single key for both encryption and decryption, therefore also called as single-Key encryption
- Symmetric Ciphers requires
  - Encryption Algorithm: Strong algorithm that produces ciphers in such a way that attackers should unable to crack the secret key
  - Secure way to share secret key: The secret key should be shared securely between the sender and receiver

The Symmetric Cipher Model

A symmetric cipher model is composed of five essential parts:

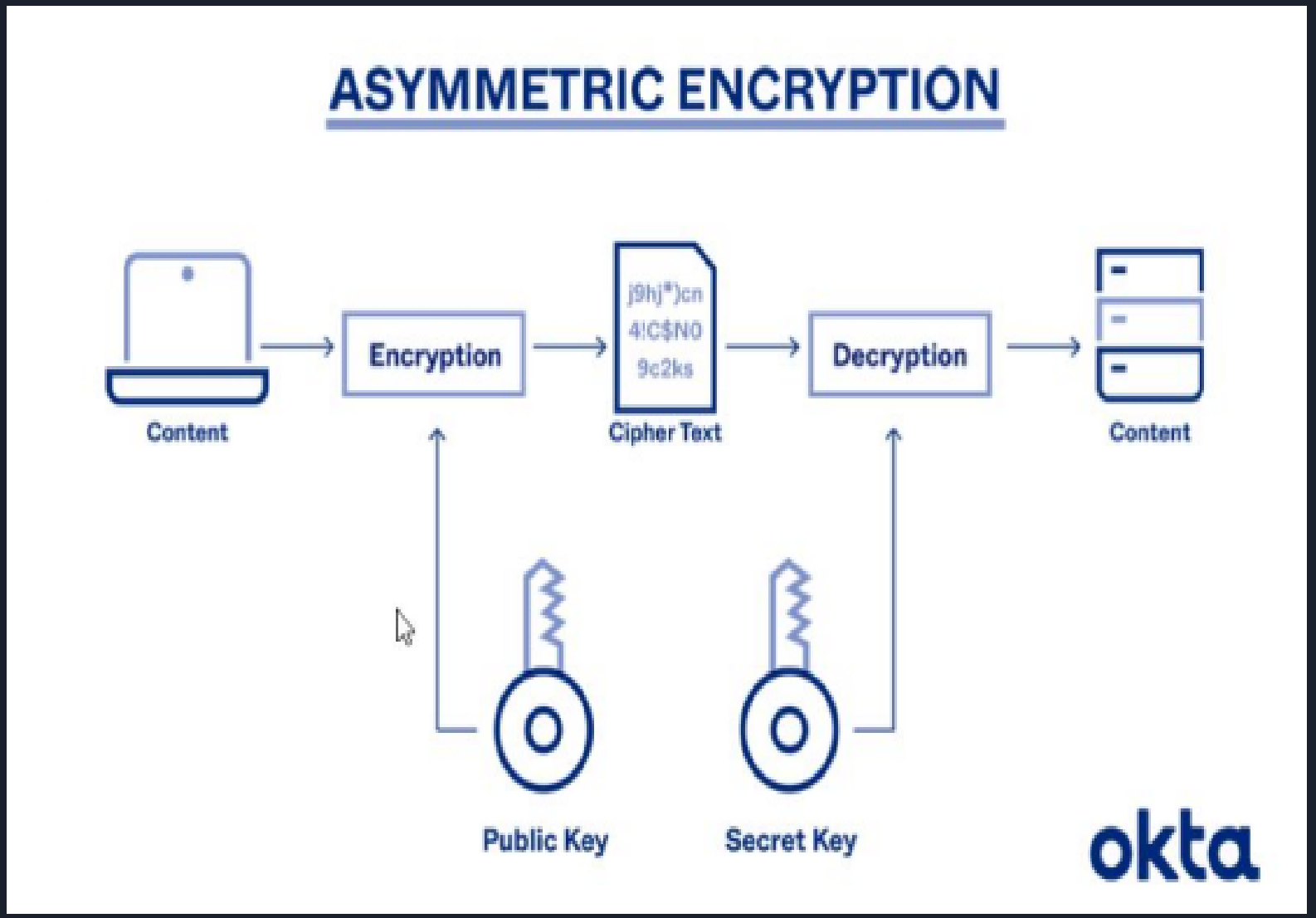


Modern Ciphers

Asymmetric Ciphers:

- It is known as public key encryption
- This encryption method contains two keys
  - Public Key: Can used by anyone to encrypt and send message
  - Private key: Have access to only one, who needs to decrypt the message

Asymmetric Cipher mechanism



Symmetric VS Asymmetric Cipher

Symmetric	Assymetric
One key used to encrypt and decrypt the message	Different keys for encryption and decrytpion
Single key is shared among all participants decreasing security	Public key is shared only to message senders. Reciptent stores private key secretly
Ciphertext size don't differ much from the original plaintext	Ciphertext is bigger than the plaintext
Very fast	Complex and slower
Usually uses 128 or 256 bits keys	Uses key which are at least 1000 bits long
Isn't used in digital signatures	It's used in digital signatures
Scalability is an issue	Easily scalable
Lack of non-repudiation	Allows non-repudiation and authenticity

Symmetric VS Asymmetric Cipher

Symmetric	Asymmetric
The Mathematical Representation is as follows- P = D (K, E(P)) where K –> encryption and decryption key P –> plain text D –> Decryption E(P) –> Encryption of plain text	The Mathematical Representation is as follows- P = D(Kd, E (Ke,P)) where Ke –> encryption key Kd –> decryption key D –> Decryption E(Ke, P) –> Encryption of plain text using encryption key Ke . P –> plain text
Examples: DES, AES, RC4 etc	Example:Diffie-Hellman, ECC, DSA and RSA

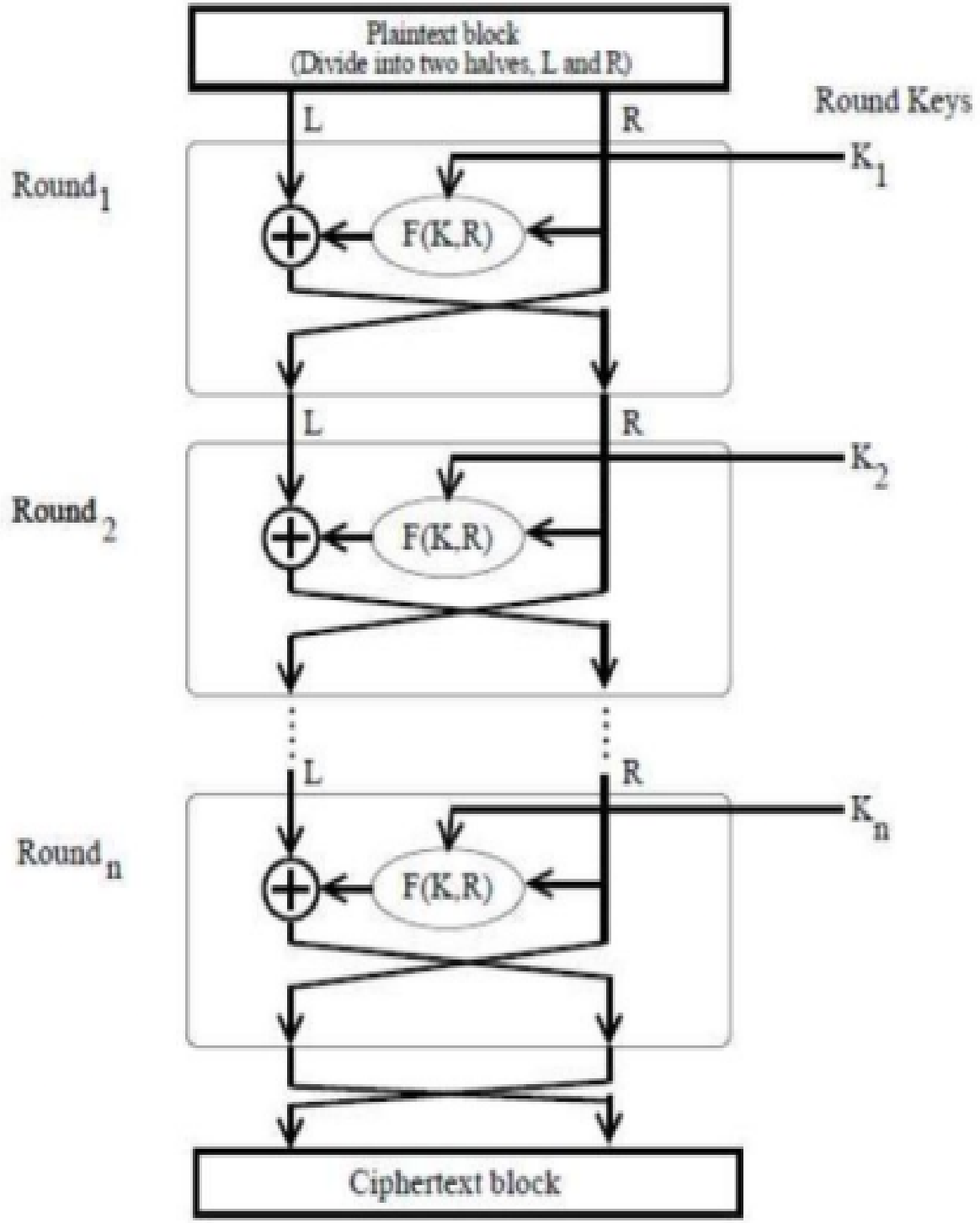
Symmetric Encryption

Feistel Cipher Structure: Feistel cipher is a design model that derives different symmetric block ciphers, such as DES. It uses same key for encryption and decryption

- Feistel cipher structure encrypts plain text in several rounds, where it applies substitution and permutation to the data.
- Each round uses different key for encryption, and same key is used for decryption process

Feistel Cipher Encryption Process

- The input block is divided into two halves that can be denoted by L and R for left and Right
- In each round, the right half goes unchanged, but left half goes through an operation that depends on R and encryption key.First we apply encryption function 'f' that takes two input -> Key (K) and (R) . The function produces output f(k,R). Then we XOR the output with L
- The Key in each round is different but is derived from the master key
- The permutation step at the end of each round swaps the modified L and unmodified R. I.E L-> R(new) , R-> L(new)
- Above substitution and permutation steps form a 'round'.
- After the completion of last round, two sub block L and R are concatenated to form cipher text

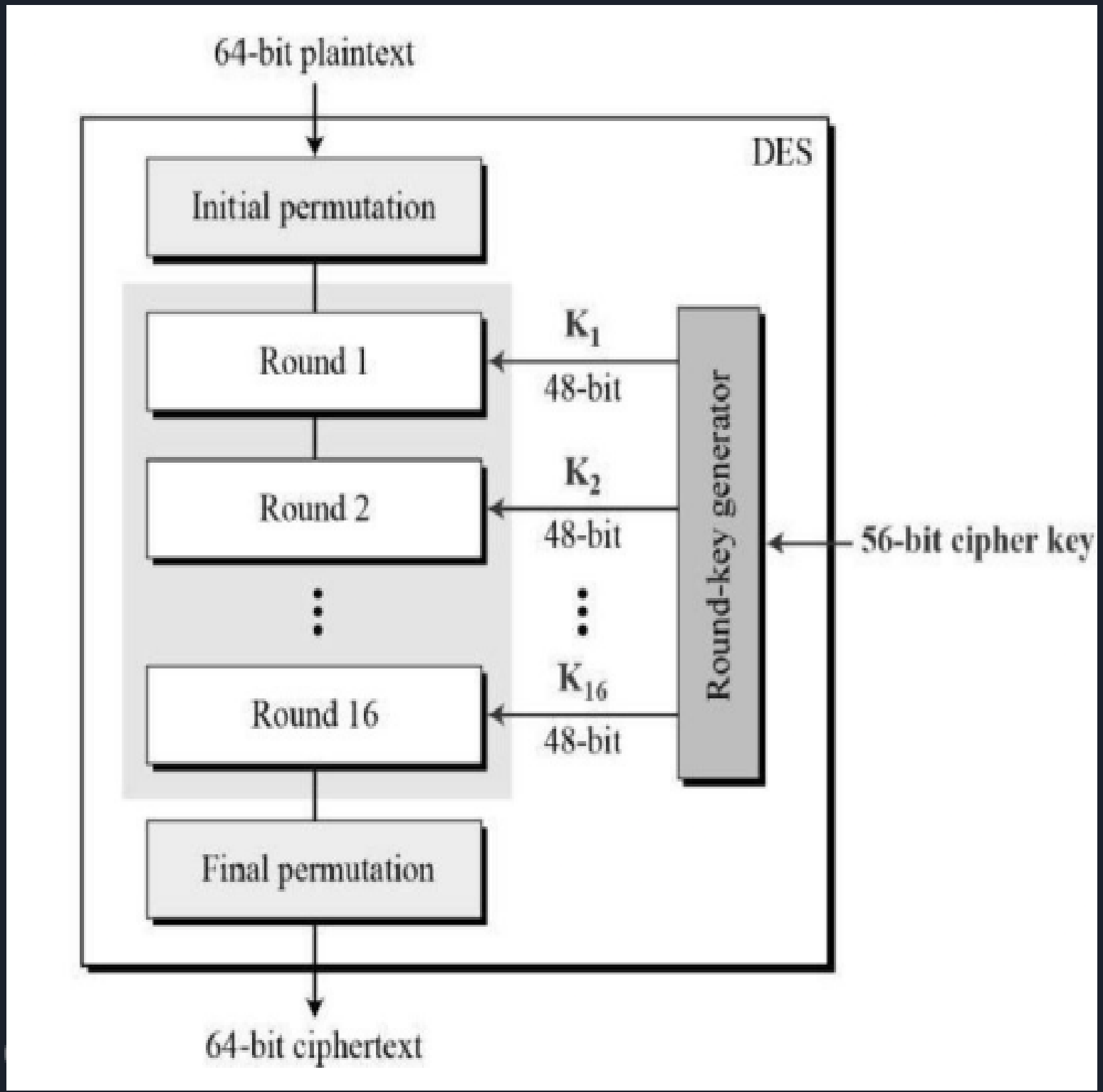


Feistel Cipher Decryption

- The decryption process is almost similar, the subkeys used in the encryption are used in reverse order
- The final swapping of L and R in last steps is crucial. If they're not swapped the resulting ciphertext couldn't be decrypted using same algorithm.

Data Encryption Standard (DES)

- DES is an implementation of Feistel Cipher.
- It uses 16 rounds feistel Structure
- DES has an effective key length of 56 bits, but actual length is 64 bits but 8 bits are not used by encryption algorithm


64-bit plaintext
DES
Initial permutation
Round 1
Round 2
Round 16
Final permutation
K_1
48-bit
K_2
48-bit
K_{16}
48-bit
Round-key generator
56-bit cipher key
64-bit ciphertext

DES

Initial Permutation:

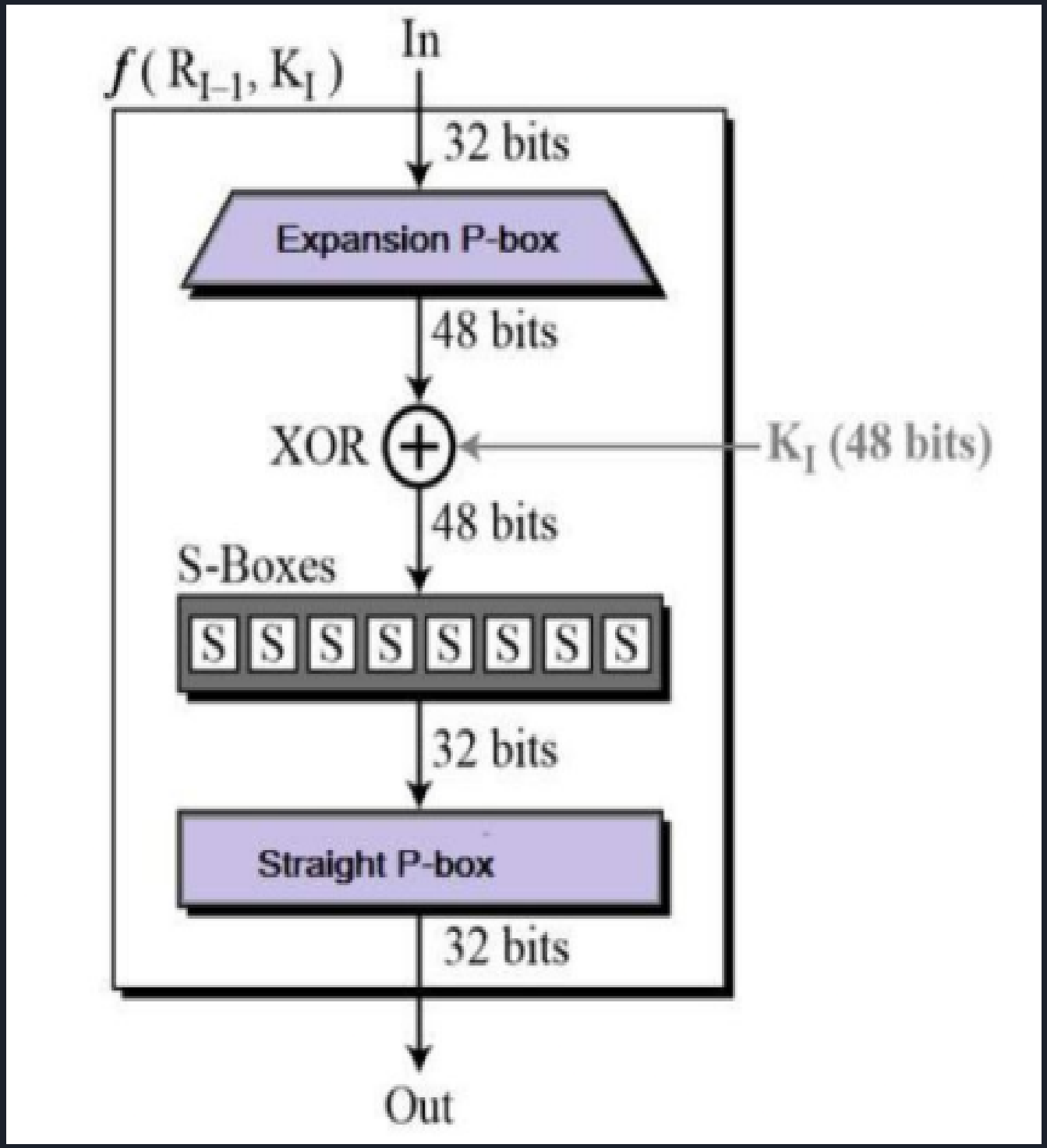
- It happens only once before the first round.
- It is nothing but the shuffling of bits position of the original plain text

After the initial permutation, the resulting 64-bits is divided into two sub block each with 32-bits and each of them run for 16 rounds

DES Function

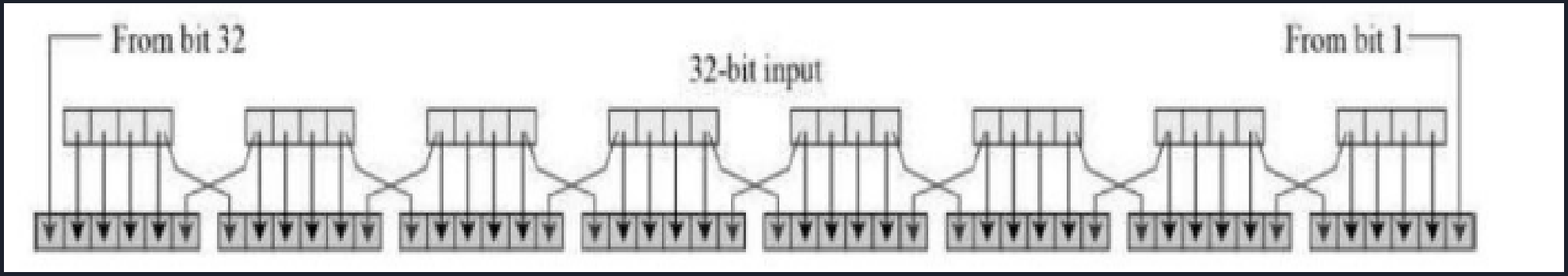
Round Function:

- It is the core of DES. The DES function uses a 48-bit key to the rightmost 32 bits to produce a 32-bit output



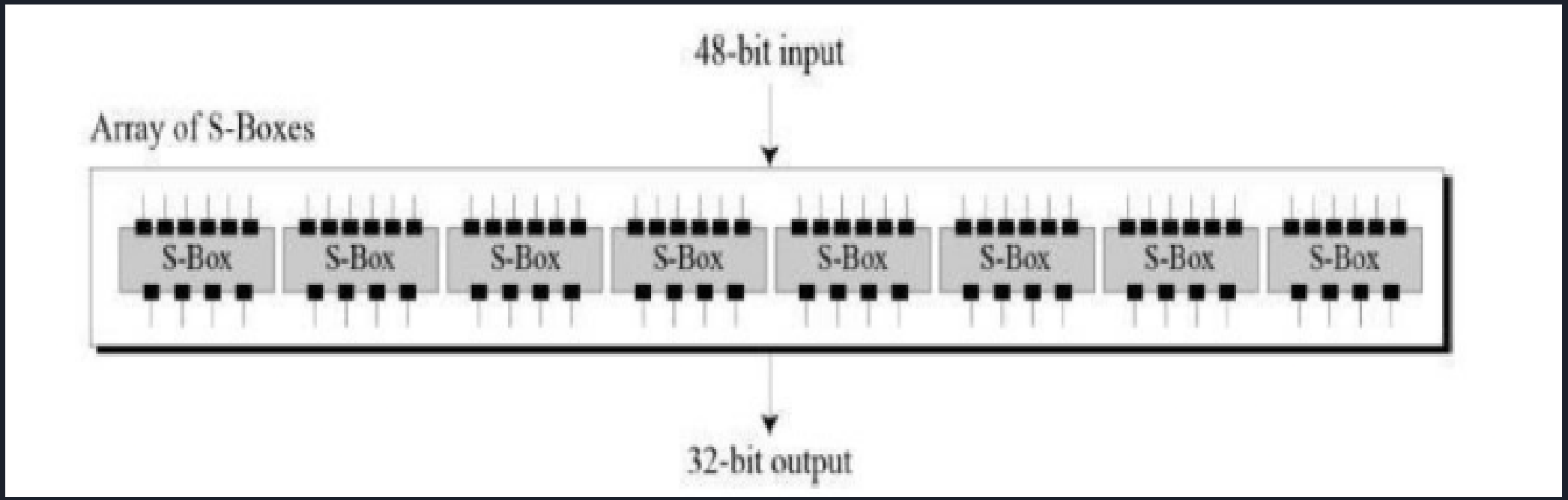
Expansion Box

Since the input is 32-bit and a round key is 48-bit, we first need to expand right input to 48-bits.
Permutation logic is explained as



DES Function

- XOR: After expansion permutation, DES does XOR operation on the expanded right section with the round key
- Substitution boxes: DES uses 8 S-boxes, each with a 6-bit input and 4-bit output



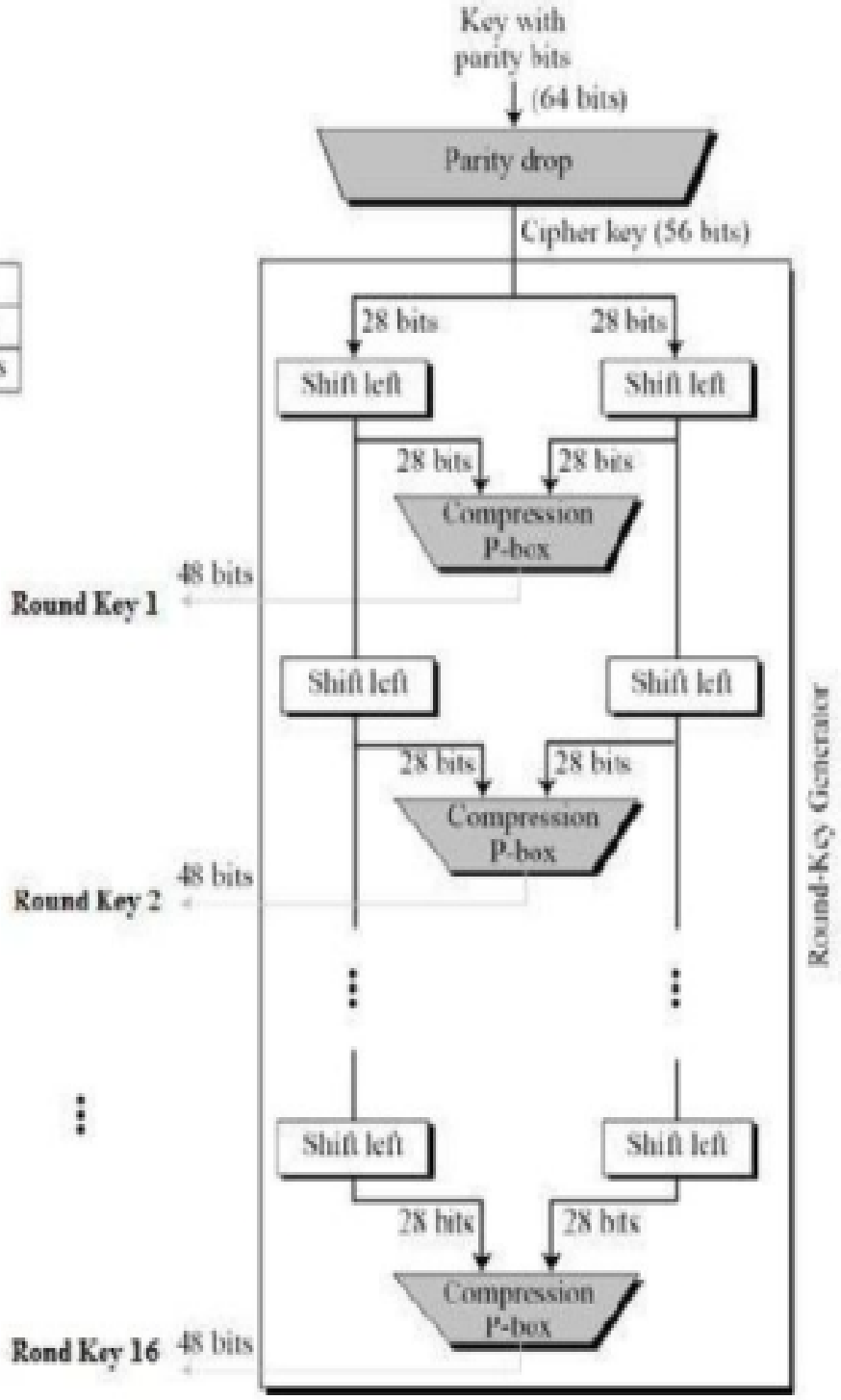
Key Generation

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

- Actually, we have 64-bit key which go as a i/p to pc-1 (permuted choice -1) and we get output as 56-bitkey
- Inside PC-I 64-bit key is divided into 8 parts each of 8 bit, and from each part last bit is discarded. -> 8,16,32 etc
- Hence we get 56-bits
- Now the 56-bit is divided into two part both of 28-bits -> C0,D0
- Now these bits are shifted with left in each rounds
- In round i=1,2,9,16 -> 1 rotated left by 1 bit
- In other rounds two halves rotated by left by 2 bits -> c1,D1
- Now C1,D1 which goes as a i/p to PC-2 which gives 48-bit
- For half C1 (8,9,22,25) and for half D1 (35,38,43,54) position bits are removed
- Thus we get our 48-bit key for round 1

Shifting

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



Basic Concepts of Fields

Groups: A group G, sometimes denoted by {G,.}, is set of elements with binary operations denoted by # that associates to each ordered pair (a,b) of elements in G an element (a.b) in G,such that following axioms are satisfied.

1. Closure: -> If a and b belongs to G, then a.b is also in G
2. Associative:-> a.(b.c)=(a.b).c for all a,b,c in G
3. Identity Element: -> There is an element e in G such that a.e = e.a =a for all a in G
4. Inverse Element: -> For each a in G, there is an element a' in G such that a.a'=a'.a=e

A group is called abelian if it satisfies the following additional condition

- Commutative: a.b = b.a for all a,b in G

Question: Is (Z, +) a group?

Solution:

Z = { ...., -3, -2, -1, 0, 1, 2, 3, ...}

CAIN Property	Explanation	Satisfied?
Closure	If a, b ∈ G, then (a • b) ∈ G.	
Associative	a • (b • c) = (a • b) • c for all a, b, c ∈ G.	
Identity element	(a • e) = (e • a) = a for all a ∈ G.	
Inverse element	(a • a') = (a' • a) = e for all a, a' ∈ G.	
Commutative	(a • b) = (b • a) for all a, b ∈ G.	

Rings

A ring R denoted by {R, +, *}, is a set of elements with two binary operations, called addition and multiplications , such that for all a,b,c ∈ R the following axioms must be satisfied.

- Group (A1-A4), Abelian Group(A5)
- Closure under multiplications (M1): If a,b ∈ R then ab ∈ R
- Associative of multiplications (M2) a(bc) = (ab)c for all a,b,c ∈ R
- Distributive laws (M3)
  - a(b+c) = ab + ac for all a,b,c ∈ R
  - (a+b) c = ac + bc for all a,b,c ∈ R

Commutative Rings: A ring is said to be commutative, if it satisfies the following additional condition:

- Commutative of multiplication (M4): ab = ba for all a,b ∈ R

Integral Domain

An integral domain is a commutative ring that obeys the following axioms:

- Multiplicative identity (M5): there is an element 1 ∈ **R such that a1=1a=a for all a ∈ R**
- **No Zero divisor (M6): if a,b ∈ R and ab=0, then either a=0 or b=0**

Fields

A fields F, sometimes denoted by {F,+,*}, is a set of elements with two binary operations, called addition and multiplication, such that for all a,b,c **∈ F, the following axioms are satisfied**

- **(A1-M6): F is an integral domain; that is, F satisfies axioms A1-A5 and M1-M6.**
- **Multiplicative inverse (M7): For each a in F, except 0, there is an element a' in F such that**

$$aa'=(a')a=1$$

Groups, Rings and Fields

Finite Fields

- A finite field or Galois field is a field that contains a finite no.of elements
- As with any field, a finite field is a set on which the operations of multiplication, addition, subtraction and division are defined and satisfy certain basic rules.
- The most common example of finite fields are given by the integer (mod p) when p is prime number

Modular arithmetic

- Modular arithmetic is a structure for integers, where numbers "wrap around" upon reaching a specific value.
- It enables us to simply make groups, rings and fields which are basic constructing piece of most modern public-key cryptography

Theorem: n is an equivalence relation on the integers. An equivalence class includes those integers which have equal remainder on division by n.

- The equivalence classes are also called a congruence classes modulo n.
- Instead of say the integers a and b equivalent and it can said that they are congruent modulo n.
- The set of all integers congruent to a modulo n is called the residue class [a].

Congruent modulo

Two integers a and b are said to be congruent modulo n if

(a mod n) = (b mod n)

This is written as a ≡ (b mod n) or b ≡ (a mod n)

Modular Arithmetic

The modulo operator has the following properties:

- $a \equiv b \bmod n$ if $n|(a-b)$
- $(a \bmod n) = (b \bmod n)$ implies $a \equiv b \bmod n$
- $a \equiv b \bmod n$ implies $b \equiv a \bmod n$
- $a \equiv b \bmod n$ and $b \equiv c \bmod n$ implies $a \equiv c \bmod n$

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

Modular arithmetic

Let Zn = {0, 1, 2,... (n-1)}, be the set of residues modulus n.

Property	Expression
Commutative laws	(w + x) mod n = (x + w) mod n
Associative laws	(w x x) mod n = (x x w) mod n
	[(w + x)+y] mod n = [w+(x+y)] mod n
Distributive laws	[(w x x) x y] mod n = [w x (x x y)] mod n
Identities	[(w x (x + y)] mod n =[(w x x) + (w x y)] mod n
	(0 + w) mod n = w mod n
Additive inverse (-w)	(1 x w) mod n = w mod n
	For each w ∈ Zn, there exists a z such that w + z ≡ 0 mod n

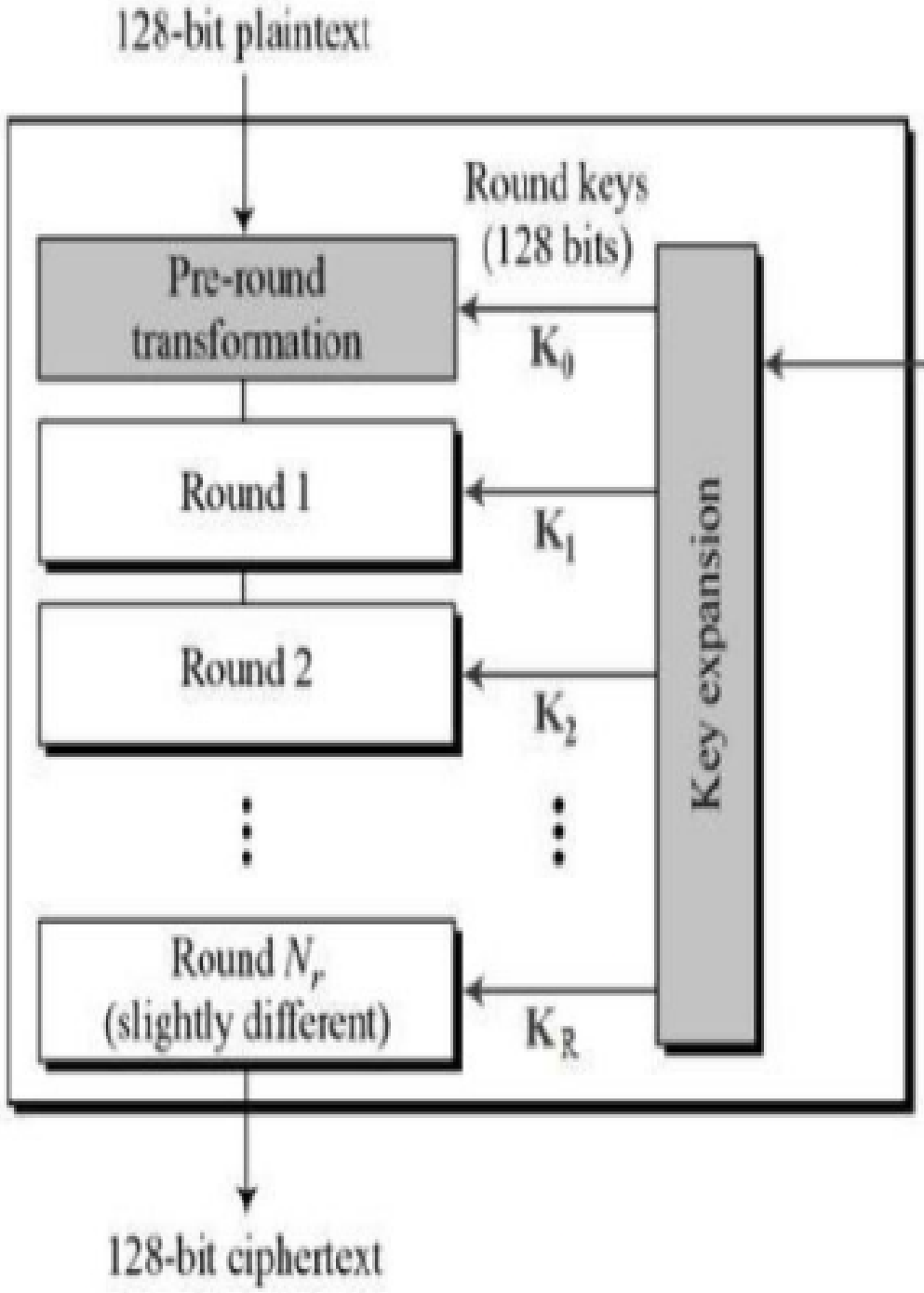
Polynomial Arithmetic

- Polynomial arithmetic in which the arithmetic on the coefficient is performed by modulo p; that is coefficient in GF(p)
- Polynomial arithmetic in which the coefficient are in GF(p), the polynomial are defined modulo a polynomial m(x) whose highest power is some integer n.

Advanced Encryption Standard (AES)

- AES is a block cipher
- The key size can be 128/192/256 for 10,12,14 rounds respectively
- Encrypts data in blocks of 128 bits each
- AES relies on substitution-permutation network principle

This means it takes 128 bits as input and output 128 bits of encrypted cipher text as output.



R	Key size
10	128
12	192
14	256

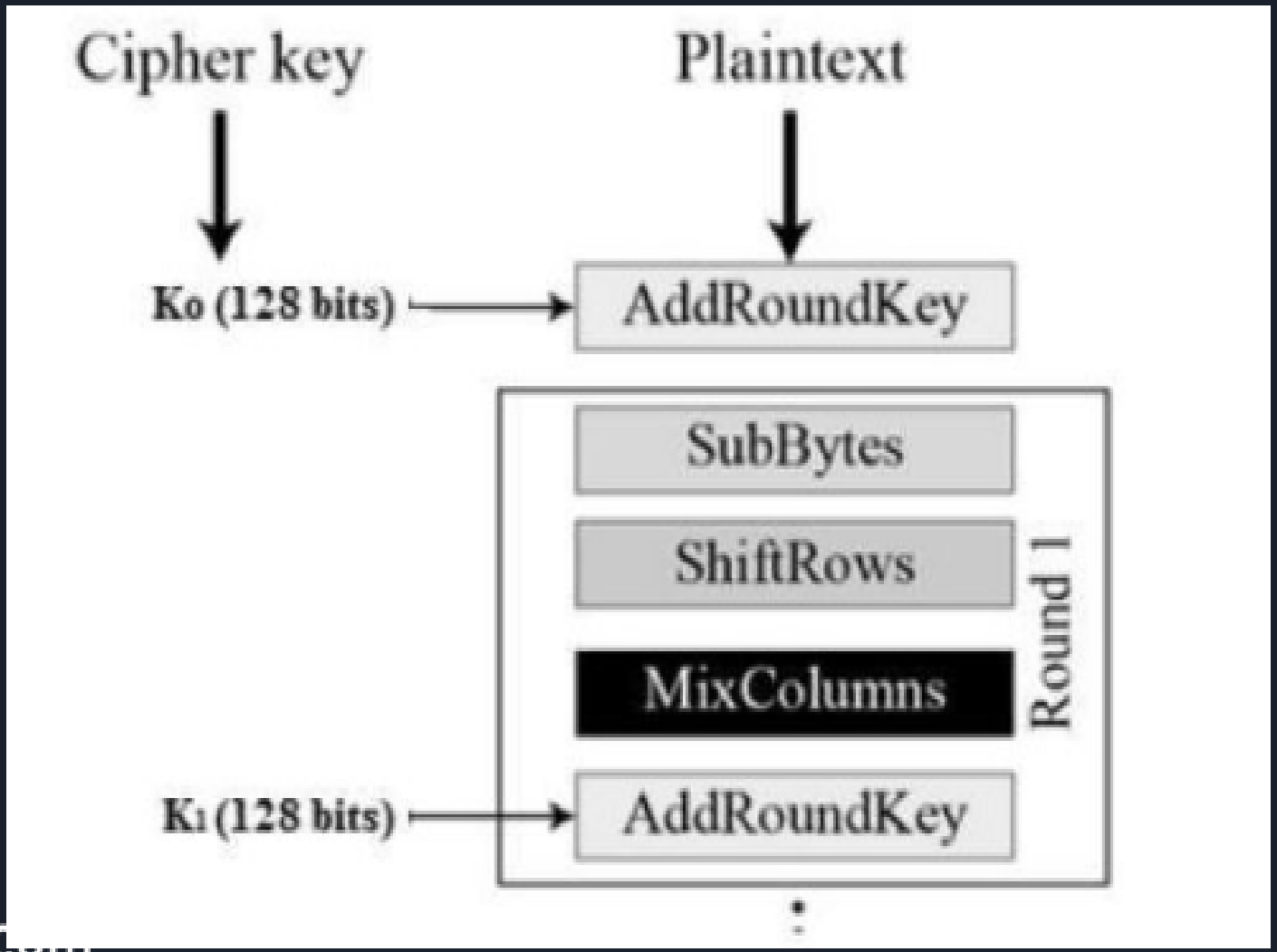
Relationship between number of rounds(R) and cipher key size

Some Terminologies

- State matrix: 4*4 intermediary output
- S-Box: 16*16 matrix of hexadecimal -> sub bytes
- Key expanding algorithm: K0-K15 -> w0-w43
- 4*4 matrix = 16 bytes = 4 word

Encryption Process (AES)

Each round comprises of four sub-processes.



AES encryption process

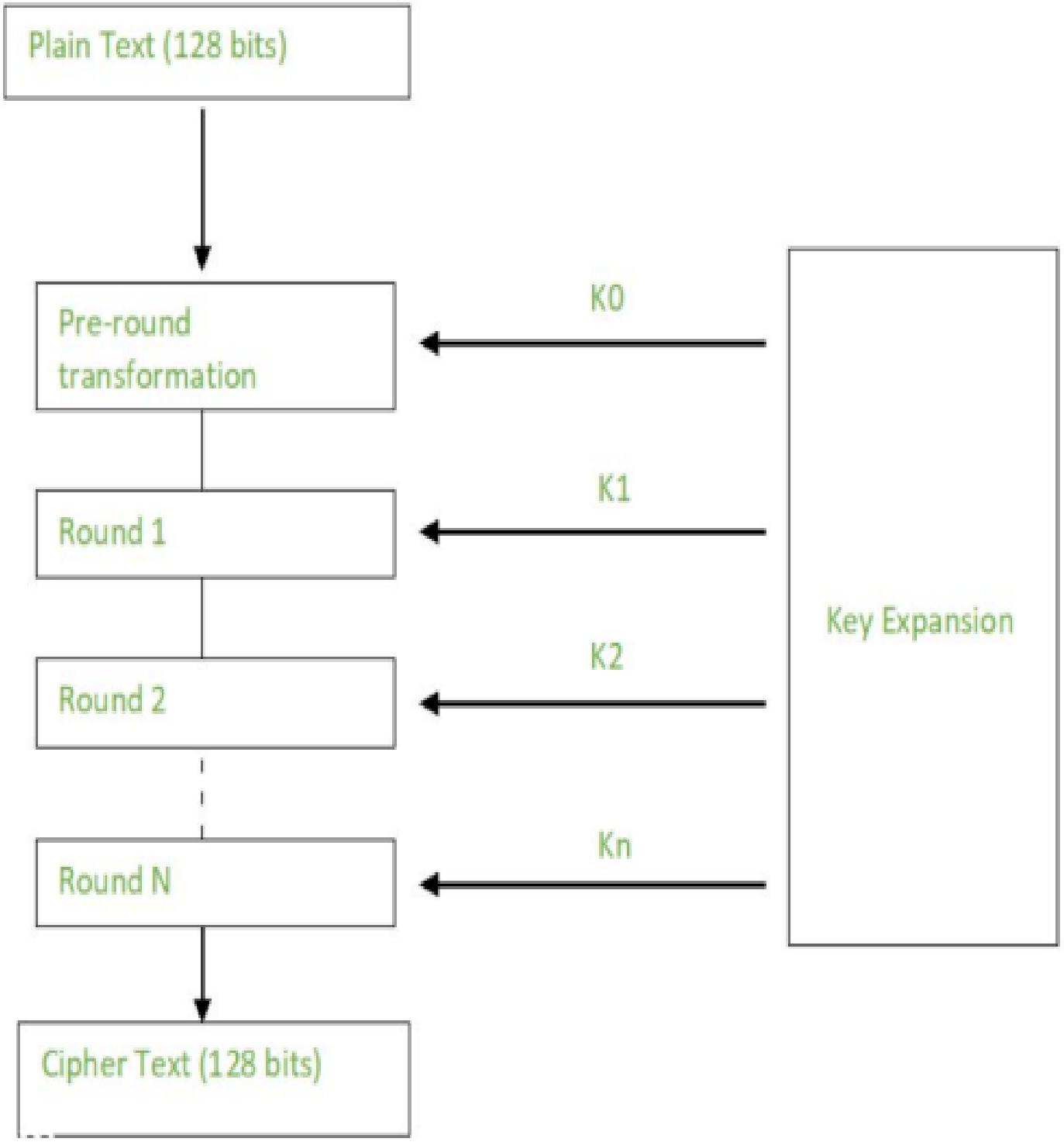
1. Byte Substitution (SubBytes): The 16 input bytes are substituted by looking up a fixed table (S-Box) given in design. The result is 4*4 matrix.
2. ShiftRows: Each of four rows of the matrix is shifted to left.
    a. First row is not shifted
    b. Second row is shifted to one byte to left
    c. Third row is shifted to two byte left
    d. Fourth row is shifted to three byte left
3. Mix Columns: Each column of four byte is now transformed using special mathematical function. This function takes an input the four bytes of one column and outputs four completely new bytes, which replaces the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

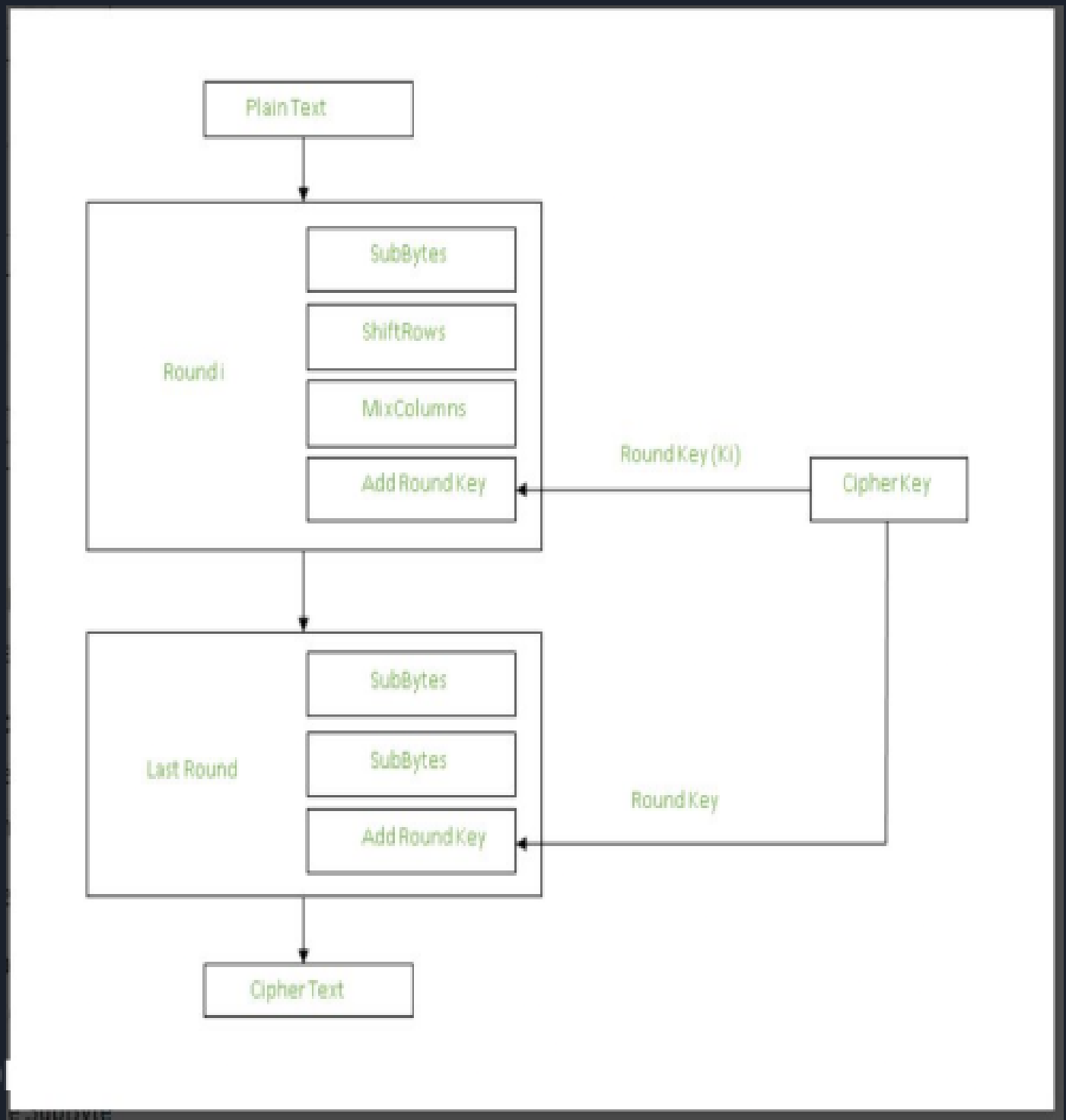
AES encryption process

4. Add Round key: the 16 bytes of matrix are now considered as 128 bits and are XORed to the 128 bits of round key. If this is last round than the output is the cipher text

Creation of Round Key (AES)

A key schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different rounds keys which will be used in corresponding round of encryption


Plain Text (128 bits)
Pre-round transformation
K0
Round 1
K1
Round 2
K2
Round N
Kn
Key Expansion
Cipher Text (128 bits)



AES Decryption process

- Add round key
- Mix column
- Shift rows
- Byte substitution

Number Theory

Prime Numbers: Prime numbers are natural numbers that are divisible by only 1 and the number itself. In other words, prime numbers are positive integers greater than 1 with exactly two factors, 1 and the number itself. For example: 2,3,5,7,11

Fermat's little theorem

Fermat's little theorem states that if p is a prime number, then for any integer a, the number a^p-a is an integer multiple of p.

Here p is a prime number

$a^p \equiv a \pmod p$

Special Case: if a is not divisible by p, Fermat's theorem is equivalent to the statement that a^(p-1) is an integer multiple of p

$a^{(p-1)} \equiv 1 \pmod p$

OR

$a^{(p-1)} \% p = 1$

Here a is not divisible by p.

Fermat's little Theorem

Example 1:

P = an integer Prime number

a = an integer which is not multiple of P

Let a = 2 and P = 17

According to Fermat's little theorem

$2^{17-1} \equiv 1 \bmod(17)$

we got 65536 % 17 ≡ 1

that mean (65536-1) is an multiple of 17

Primality Testing

Primality test: It is an algorithm for determining whether an input number is prime or not.

Miller-Rabin Primality Test:

1. Perform n-1 such that n-1 = m * 2^k (find the value of m and k)
2. If k<=1;

   Calculate T such that T = a^m mod n; if T = (+-1), it is prime, else composite

3. If k> 1; calculate T such that T= T^2 mod n ,

   if (T = 1) Composite

   If (T= -1) prime

   Else

   Composite

Miller-Rabin primality test

Is 53 a prime number? a=2.

1. N-1 = m*2^k

   m =13, k=2

2. T = T^2 mod n; T= a^m mod n

   (a^m mod n)^2 mod n = (2^13 mod 53)^2 mod 53 = (30)^2 mod 53 = 900 mod 53= 52

3. Since T = -1 than n, therefore . 53 is a prime number

Euclidean Theorem

Used to determine the GCD (Greatest Common Divisor) of two positive integers

- gcd(a,b) = gcd (b, a mod b)
- gcd(a,0) = a

Find the GCD(12, 33).

Q	A	B	R
2	33	12	9
1	12	9	3
3	9	3	0

- GCD(15,45) ?

$a = 15 \quad b = 45$

$gcd(a, b) = gcd(b, a \bmod b)$

$= gcd(45, 15 \bmod 45)$

$= gcd(45, 15)$

$a = 45, \; b = 15$

$gcd(45, 15) = gcd(15, 45 \bmod 15)$

$= gcd(15, 0) = 15$

Extended Euclidean algorithm

It is an extension of euclidean algorithm which is also used to find out the multiplicative inverse.

In first step; we assume T1=0, T2=1 ; T = T1-T2*Q;

If no further operation can be performed we get the multiplicative inverse as T1

Multiplicative Inverse using EEA

Example 1: What is the multiplicative inverse of 3 mod 5.

Q	A	B	R	T_1	T_2	T
1	5	3	2	0	1	-1
1	3	2	1	1	-1	2
2	2	1	0	-1	2	-5
X	1	0	X	2	-5	X

∴ 2 is the M.I of 3 mod 5.

Euler's Totient function

Relatively prime: When two numbers have no common factors other than 1, they are said to be relatively prime. In other words, no number other than 1 can divide them both exactly (without any remainder)

Euler's Totient function

- Denoted by Φ(n).
- Φ(n) = Number of positive integers less than 'n' that are relatively prime to n

Euler's Totient Function

Example 1: Find Φ(5).

Solution:

Here n=5.

Numbers less than 5 are 1, 2, 3 and 4.

GCD	Relatively Prime?
GCD (1, 5) = 1	
GCD (2, 5) = 1	
GCD (3, 5) = 1	
GCD (4, 5) = 1	

Asymmetric Encryption

Diffie-Hellman Key Exchange:

The diffie-hellman algorithm is being used to establish a shared secret that can be used for secret communication while exchanging data over public network.

Algorithm

1. Consider a prime number 'q'
2. Select **'α'** such that it must be primitive root of q and **'α'< q**

'a' is a primitive root of q if ;

a mod q , a^2 mod q, …… a^(q-1); gives result

{1,2,3,....q-1}

I.e. Value shouldn't be repeated and we should have all the value in the output set from 1 - (q-1)

Diffie-hellman example

Let q = 7

Calculating primitive root.

Let us assume a= 5 which is less than 7

5^1 mod 7 = 5

.

.

5^6 mod 7 = 1

Therefore '**α**' **= 5**

Here '**α**' , q -> global public elements (known to everyone)

Diffie-hellman example

X-> private key of users

Y-> public key of users

3. Assume Xa (private key) and Xa < q

   Calculate: Ya = **α**^Xa mod q

4. Assume Xb private of B and Xb < q

   Calculate: Yb = **α**^Xb mod q

Diffie-hellman

Now we will calculate secret key

To calculate the secret key both the sender will use the public key

$K_a = (Y_b)^{Xa} \bmod q$

$K_b = (Y_a)^{Xb} \bmod q$

$k_a = k_b$; the key is exchanged successfully

Example:

```
Step 1: Alice and Bob get public numbers P = 23, G = 9

Step 2: Alice selected a private key a = 4 and
        Bob selected a private key b = 3

Step 3: Alice and Bob compute public values
Alice:    x =(9^4 mod 23) = (6561 mod 23) = 6
        Bob:    y = (9^3 mod 23) = (729 mod 23)  = 16

Step 4: Alice and Bob exchange public numbers

Step 5: Alice receives public key y =16 and
        Bob receives public key x = 6

Step 6: Alice and Bob compute symmetric keys
        Alice:  ka = y^a mod p = 65536 mod 23 = 9
        Bob:    kb = x^b mod p = 216 mod 23 = 9

Step 7: 9 is the shared secret.
```

RSA Algorithm

- It is an asymmetric cryptographic algorithm. I.e. public key and private key
- If public key of user A is used for encryption, we have to use the private key of same user for decryption
- The RSA scheme is a block cipher in which the plain text and cipher text are integers between 0 and n-1 for some value n.

1. Key Generation

A. Select two large no. 'p' and 'q'
B. Calculate n = p*q
C. Calculate Φ(n) = (p-1)*(q-1) // euler totient function
D. Chose value of 'e'

$1 < e < \Phi(n)$ and GCD $(\Phi(n), e) = 1$

E. Calculate

$d = e^{-1} \bmod \Phi(n)$

$ed = 1 \bmod \Phi(n)$

$ed \bmod \Phi(n) = 1$

Key Generation

F. Public key = {e,n}

G. Private key = {d, n}

RSA

2. Encryption:

$$C = M^e \bmod n$$

3. Decryption

$$M = C^d \bmod n$$

RSA example

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and φ (n) are coprime. Let e = 7
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

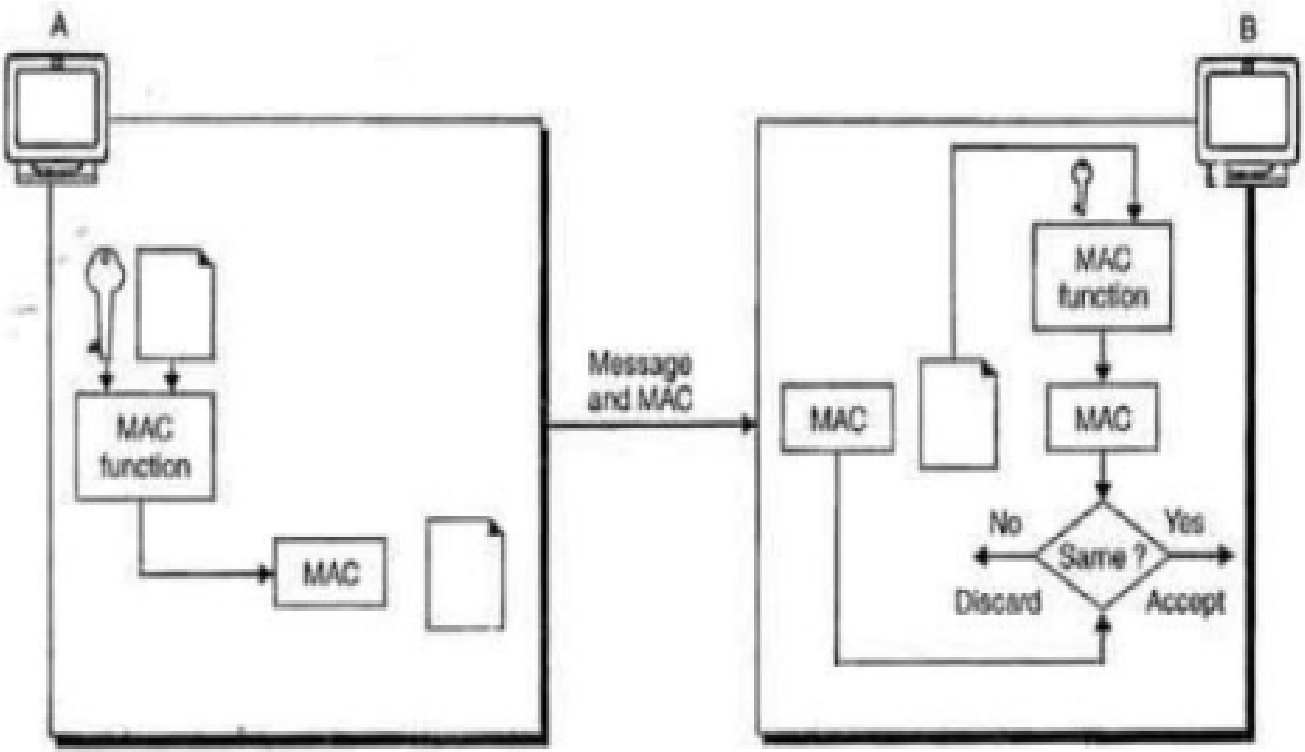
Chapter 3

MESSAGE AUTHENTICATION AND HASH FUNCTION

Message Authentication

- Message authentication ensures that the message has been sent by a genuine identity not an imposter
- The service used to provide message authentication is Message Authentication Code(MAC)
- This system make use of symmetric key shared by A and B
- A, Using this symmetric key and a keyed hash function, generated MAC
- A then sends this MAC along with the original message to B
- B receives the message and the MAC and separates the message from the MAC
- B then applies the same keyed hash function to message using the same symmetric key to get fresh MAC
- B then compares the MACs sent by A with the newly generated MAC
- If the two MACs are identical, it shows the messages hasn't been modified

Message Authentication Code



MAC created by A and checked by B.

HASH FUNCTION

- Similar to MAC but it doesn't uses key
- Takes variable size message and produce a fixed output called hash code/hash value
- The only input is the message
- A hash value 'h' is generated by a fn H

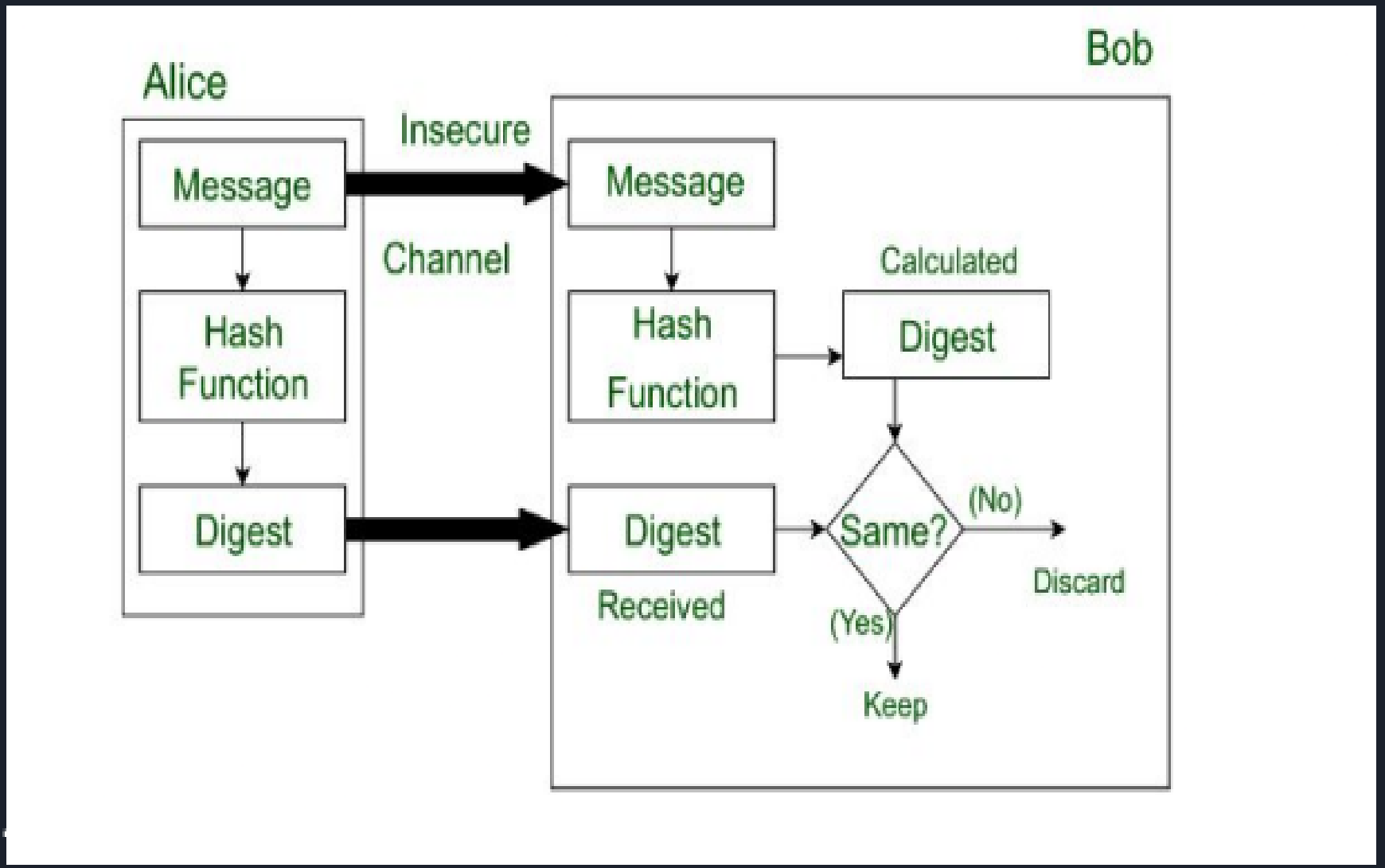
H(M) = fixed length code 'h'

- They are also called compression function

Message Digest MD

- It is used to ensure the integrity of a message transmitted over an insecure channel (where the content of message can be changed). The message is passed through a cryptographic hash function. This function creates a compressed image of the message called digest.
- The digest should be unchanged during the transmission
- The cryptographic hash function is one way function, which means, a function which is infeasible to invert. This hash function takes a message of variable length as input and creates digest/ hash/ fingerprint of fixed length, which is used to verify the integrity of message
- Message digest ensures the integrity of the document. To provide authenticity of message, digest is encrypted with sender's public key. Now this digest is called digital signature, which can only be decrypted by the receiver who has sender's private key. Now the receiver can authenticate the sender and also verify the integrity of message sent.

Message Digest



MD4

- This is for 32 bits computers.
- Hash function which digest an arbitrary length message of 128 bits

Working principle of MD4

- The original message must be congruent to the 448 modulo 512 which is 448
- If the message is not equal to 448 modulo 512, then we'll add 1 followed by 0 until it becomes congruent to 448. Eg. for aba -> aba10000000 till it became congruent to 448 modulo 512
- Now the padded message length is a multiple of 512 bits, which is the block size used by MD4 hash function.
- Finally we'll add 64-bit representation of the original message length . aba100.....0000
- This final padded message is then processed by the MD4 function to produce message digest
- Now after digest the output is 128 bit

MD 5

- md5 is a cryptographic hash function algorithm that takes message as input of any length and changes it into fix-length of 16 bytes.
- It was developed as an improvement as MD4, with advanced security
- The output of MD5 (Digest Size) is always 128 bits

Usage of MD5 Algorithm

- It is used in file authentication
- In a web application, it is used for security purpose. E.g. secure password of users
- Using this algorithm, we can stored our password in 128 bits format

Working of MD5

1. **Append the Padding bits:** In first step, we add padding bits in the original message in such a way that the total length of message is 64 bits less than exact multiple of 512.

   Length(original message + padding bits) = 512 * i – 64 where i = 1,2,3 . . .

2. **Append the length bits:** In this step, we add the length bit in the output of the first step in such a way that the total number of the bits is perfect multiple of 512. Simply, here we add the 64-bit as a length bit in the output of the first step.

   I.e output of first step = 512*n - 64

   Length bits = 64

   After adding we will get 512*n, the exact multiple of 512

Working of MD5

3. **Initializing MD buffer:** Here, we use the 4 buffers, I.e. J,K,L,M. The size of each buffer is 32 bits

- J = 0x67425301
- K = 0xEDFCBA45
- L = 0x98CBADFE
- M = 0x13DCE476

Working of MD5

4. **Process each 512-bit Block:**

- This is the most important step of MD5 algorithm
- Total of 64 operations are performed in 4 rounds.
- First round 16 operations will be performed, second round 16, third round 16, fourth round 16 operations are performed
- We apply different function for each rounds as F, G, H, I respectively
- AND, OR, XOR and NOT operations are used to calculate functions with three of the buffer . I.e. K,L,M

  - F(K,L,M) = (K AND L) OR (NOT K AND M)

  - G(K,L,M) = (K AND L) OR (L AND NOT M)

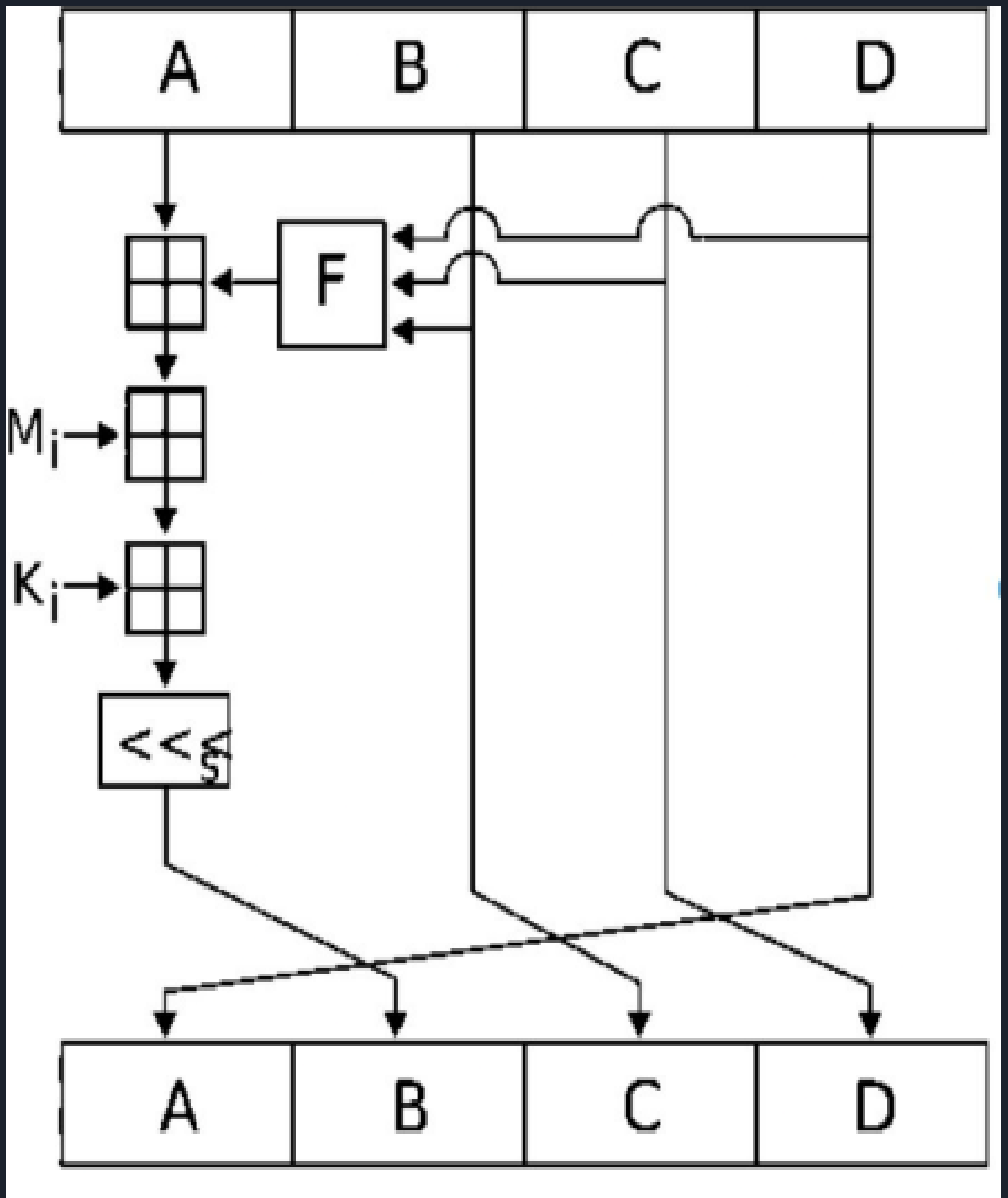
  - H(K,L,M) = K XOR L XOR M

  - I(K,L,M) = L XOR (K OR NOT M)

Working of MD5

After applying the function now we perform an operation on each block. For performing operations we need

- Add modulo 2^32
- M[i] - 32 bits message
- K[i] - 32 bits constant
- <<<n - Left shift by n bits



Secure hashing Algorithm(SHA 1)

- It is the upgrade of SHA
- It gives the output of 160 bits while MD5 gives of 128 bits
- It's input data is also of 512 bits

SHA 1 Working

- **Append the padding bits:** The original message is padded and its duration is congruent to 448 modulo 512. Padding is continually inserted up-to the desired length.Padding includes single 1 followed by essential numbers of 0 bits.
- **Append length:** A 64-bit block considered as a unsigned 64-bit integer(most essential byte first), and defining the length of original message is added to the message. The complete message length is a multiple of 512
- **Initialize the buffer:** The buffer includes five register each of 32 bits indicated by A,B,C,D,E. The 160-bit buffer can be used to influence temporary and final outcomes of the compression function
    - A = 67 45 23 01
    - B = ef cd ab 89
    - C = 98 ba dc fe
    - D = 10 32 54 76
    - E = c3 d2 e1 f0

SHA 1 working

Process message in 512-bit blocks: The compression function is divided into 20 sequentials steps includes four rounds of processing where each round is made of 20 steps.

- The four rounds are structurally same as one another with only difference that each round need a different Boolean function, which is defined as f1,f2,f3,f4 and one of four multiple additive constant Kt (0<=t<=79).

Output: After processing the final 512-bit message block , we get the output of 160 bit message digest

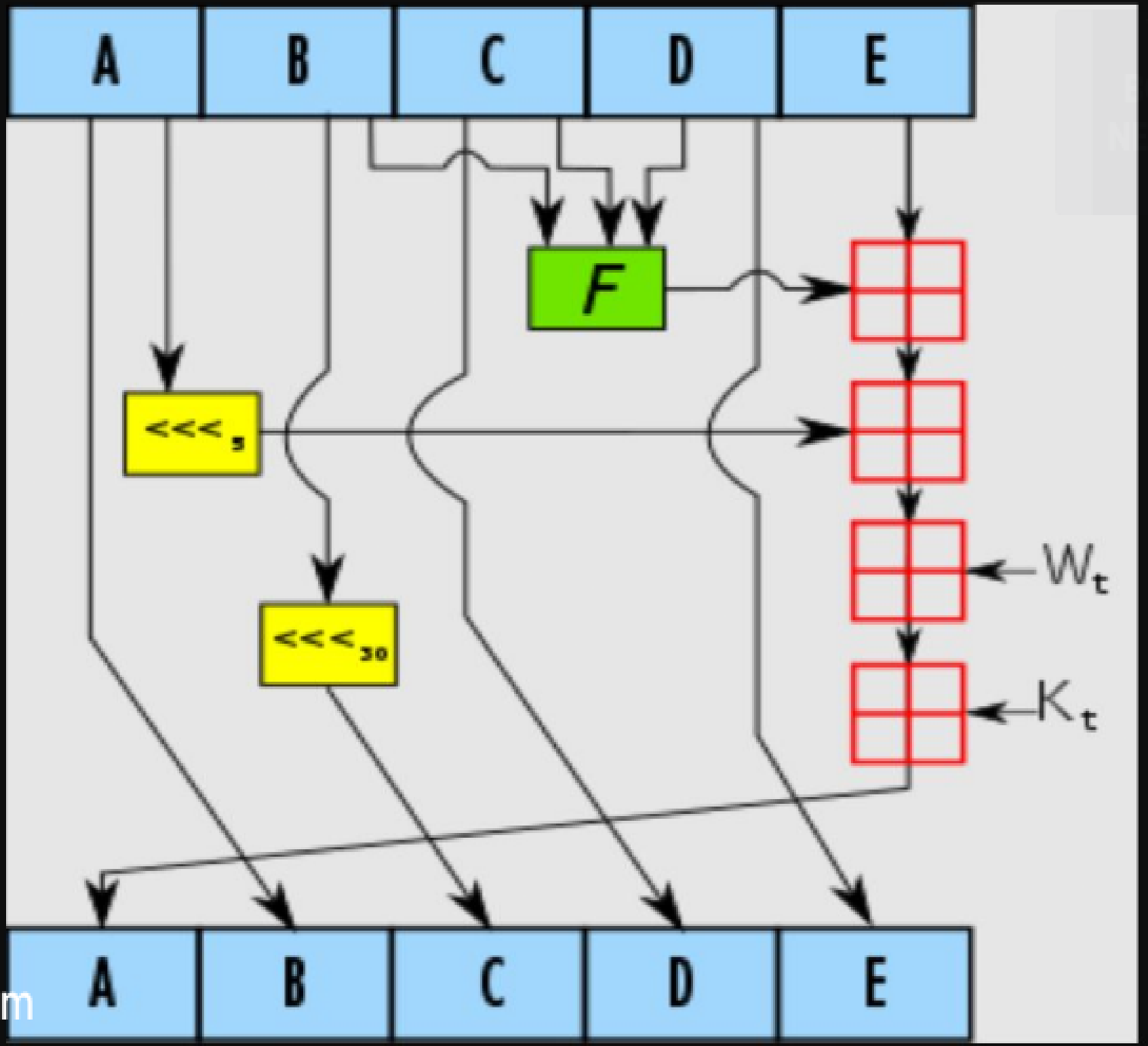
SHA 1 working

F(t,B,C,D) = (B AND C) OR ((NOT B) AND D)

F(t,B,C,D) = B XOR C XOR D

F(t,B,C,D) = (B AND C) OR (B AND D) OR (C AND D)

F(t,B,C,D) = B XOR C XOR D



Difference MD5 and SHA 1

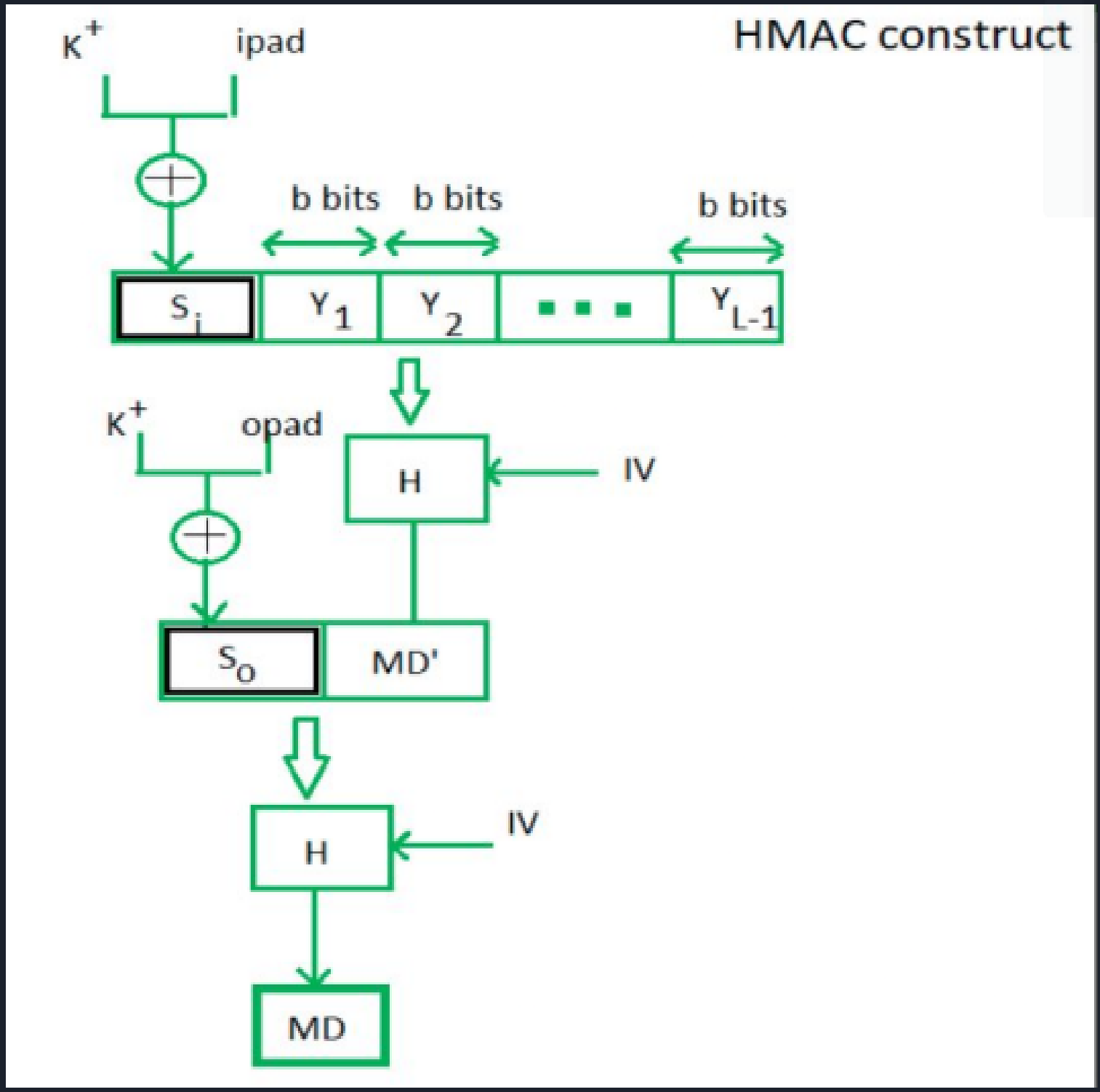
- MD5 performs 64 operations and SHA-1 performs 80 operations.
- The vector K changes within a round in MD5 and it is fixed for the whole round in SHA-1.
- The shift is fixed to 5 in SHA-1 and it changes in MD5.
- In one operation MD5 changes only one word from the Initial Vector and SHA-1 change two of them.
- MD5 produces 128 bits digest using an Initial Vector of four 32-bits words and SHA-1 produces 160-bits digest using an Initial Vector of five 32-bits words.

HMAC (hash based message authentication code)

- HMAC is a type of message authentication code (MAC) that is acquired by executing a cryptographic hash function on the data that is to be authenticated and a secret shared key.
- Like other MAC, it is used for both data integrity and authentication

Working of HMAC

- Message M containing blocks of length b bits.
- An input signature is padded to the left of the message and the whole is given as input to a hash function which gives a temporary MD.
- MD again is appended to an output signature and the whole is applied hash function again
- The result is our final MD



Working of HMAC

- Here, H stands for Hashing function,
- M is the original message
- Si and So are input and output signatures respectively,
- Yi is the ith block in original message M, where I ranges from [1, L)
- L = the count of blocks in M
- K is the secret key used for hashing
- IV is an initial vector (some constant)
- The generation of input signature and output signature *Si* and *So* respectively.

Working of HMAC

$S_i = K^+ \oplus ipad$ where K^+ is nothing but K padded with zeros on the left so that the result is b bits in length

$S_o = K^+ \oplus opad$ where ipad and opad are 00110110 and 01011100 respectively taken b/8 times repeatedly.

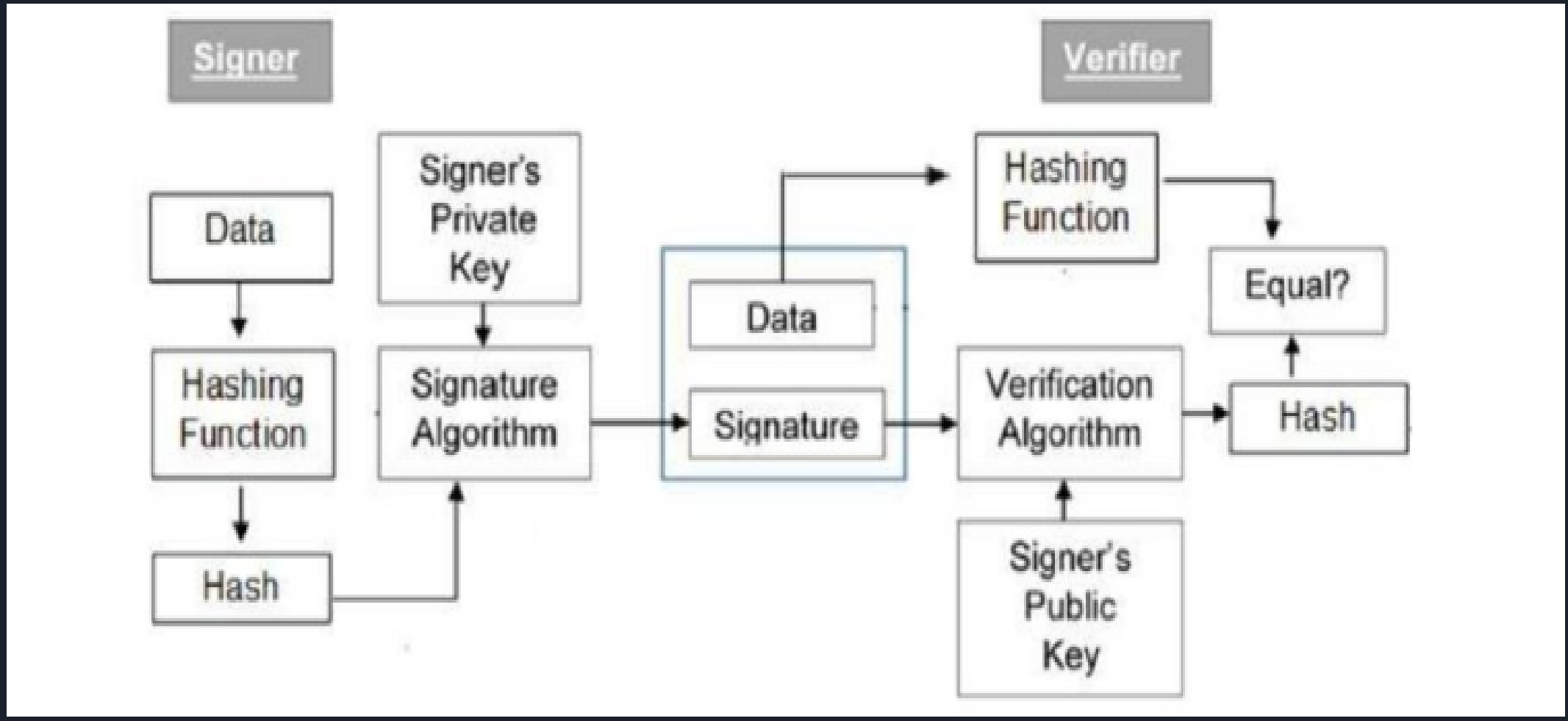
$MD' = H(S_i || M)$

$MD = H(S_o || MD')$ or $MD = H(S_o || H(S_i || M))$

Digital Signatures

- Digital signature is a techniques that binds a person/entity to digital data. This binding can be independent verified by the receiver as well as third party
- Digital signature is a cryptographic value that is calculated from the data and a secret key known only to signer
- In real world the receiver of message needs assurance that the message belong to the sender. This requirement is very crucial in business application

Model of digital signatures



Digital Signature

- Everyone using this scheme has public private key pair
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as signature key and public key as verification key
- Signer feeds data to the hash function and generated the hash of data
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier
- Verifier feeds the digital signature and verification key into verification algorithm. The verification algorithm gives some value as output.
- Verifier also run same hash function on received data to generate hash value
- For verification, this hash value and output of verification algorithm are compared. Based on comparison results, verifier decides whether the signature is valid
- Since digital signature is created by private key of signer and no one else can have this key;the signer cannot repudiate signing the data in future

CHAPTER 4

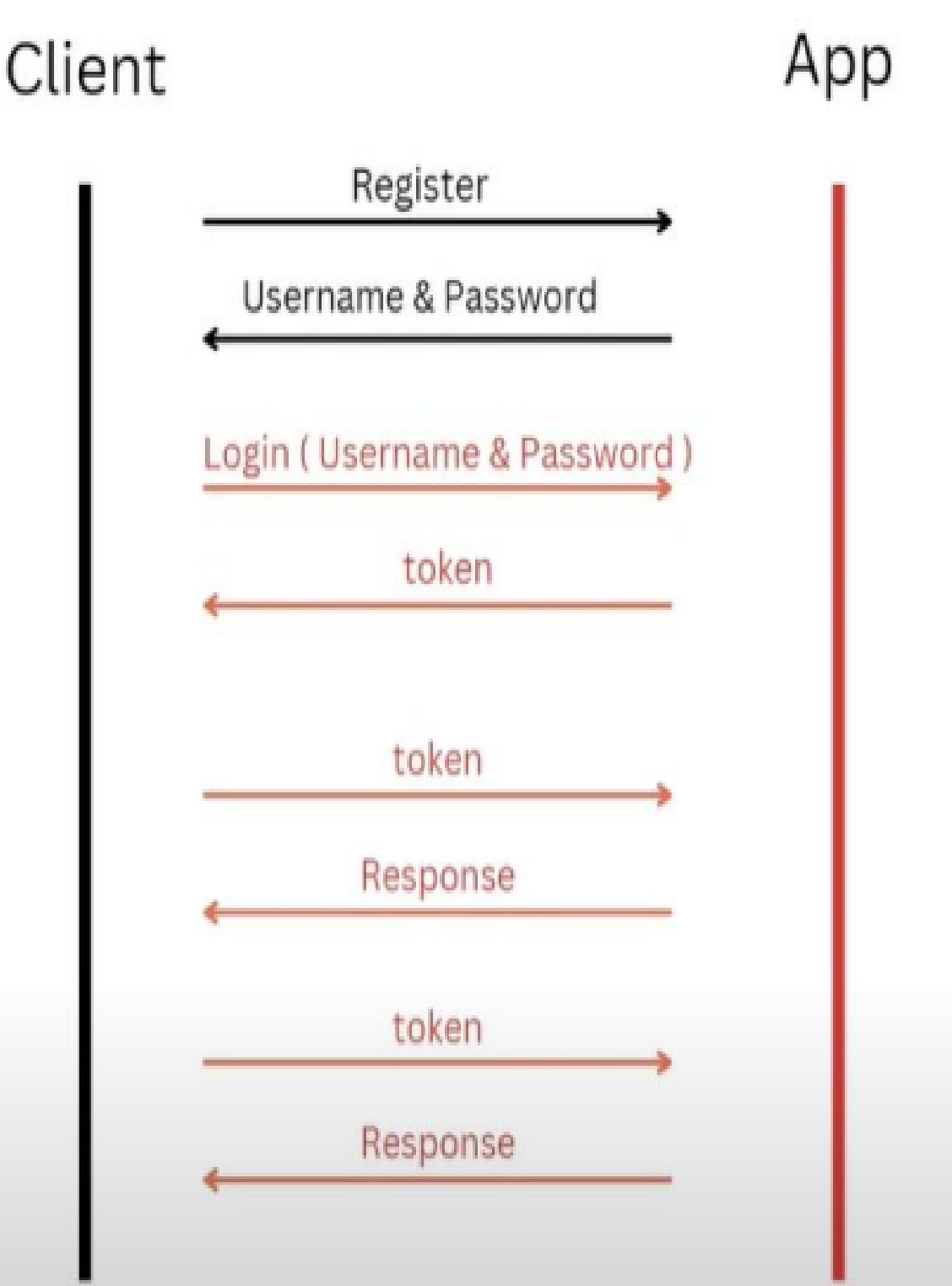
User Authentication

Types of Password based authentication

a. Store password in plain text: Store password in plain text and used the password for authentication purpose
b. Derived from password: In this type, the server first encrypt the password before storing to the database and uses the same encryption algorithm to compare the password and if matched, then only the users will be authenticated
c. Message digest password: In this type, the message digest is used to create a digest of password and store in the database, and compare the hash using same hashing function to compare if the authentication should be granted or not.

Token based authentication

- Token based authentication is a protocol which allows users to verify their identity, and in return receive a unique access token.
- During the life of token, users then can access the website or app that the token has been issued for, rather than having to re-enter credentials each time they go back to same web page or app
- The user retain access as long as the token remains valid.Once the user logs out or quits app, the token is invalidated
- It provides a second layer of security and administrators have detailed control over each action and transaction
- The token implementation is quite hard so developer might consider all edge cased before it is implementing it.
- JWT is one of the example of token based authentication



Token Authentication Types

1. **Connected:** Keys, discs, drives, and other physical items plug into system for access. Eg. smartcard
2. **Contactless:** A device is closed enough to server to a communicate with, but it doesn't plug in. Microsoft "magic-ring" would be an example of it.
3. **Disconnected:** A device can communicate with the server across long distances, even if it never touches another devices at all. E.g. two factor authentication

Working of Token based authentication

- **Request:** The person ask for access to server or app. This could involve login with password or any other methods
- **Verification:** The server determines that the person should have the access. It involves like checking the password provided by the user.
- **Tokens:** The server communicates with authentication device, like ring, key, phone. After verification, the server issues a token and passes it to users.
- **Storage:** The token sits within the user's browsers while work continues

Biometric authentication

- Biometric authentication refers to the security procedure that involves the use of unique biological characteristics of individuals such as retinas, voices, facial characteristics and fingerprints in order to verify people who they claim to be.
- This process is used to control access to physical and digital resources, such as buildings, rooms and different devices.

Types of Biometric

1. Physical biometrics:
    a. Fingerprints
    b. Facial recognitions
    c. Iris and retinas
    d. Voice recognitions
    e. DNA
2. Behavioral biometrics:
    a. Signatures
    b. Behavioral characteristics of persons like walking, speaking styles, postures etc

Criteria for selection of Biometric

- Universality: Each person should possess the biometric traits which is being used.e.g facial recognitions
- Uniqueness: No two persons must be same in terms of biometric traits being used. I.e everyone must be unique in terms of biometric terms used.
- Permanence: It should be invariant over time. I.e it should changed over time
- Collectability: Biometric traits must be easily measurable
- Performance: Processing of biometric must be easy and fast
- Secure: It must be secure and can't be copied
- Acceptability: People should be willing to accept the biometric system

Advantages of biometric

- **Invariant:** Biometric traits are invariant over time as smart cards get damaged over time but biometric traits doesn't.
- **Accountability:** If there is a security breach, then biometric ensures who can be the responsible person for the breach but in traditional methods, smart cards can be stolen and used by someone else. Hence, accountable person is easily identifiable nowadays by using biometric.
- **Easy to use:** Biometric systems are easy to use.
- **Convenient:** User doesn't have to remember passwords, pins and keep safe the smart cards like before.
- **More secure:** Biometric trait can't be stolen or copied

Remote user Authentication

- Remote user authentications is the process of verifying the user remotely to grant access to the organization's system or network

How does Remote user Authentication works

1. **Identification:** The user need to perform certain identity verification activities like face authentication, password authentications, fingerprint scan etc using some of the tools and softwares
2. **Verifications:** In this steps, the information generated is matched with records to confirm identity presented at step 1

Remote user authentications

The means of authentications are

1. User knowledge: passwords, answers to specific questions, PIN or OTP
2. Organization-issued assets: Smart card, cryptographic keys, physical keys
3. Biometric features: face, retina, fingerprints etc
4. Biometric characters: Voice recognitions, typing rhythms, handwritings etc

Remote user authentication advantage

1. Quick Access:
2. Cost effective:
3. Secure:
4. Private
5. Convenience

Drawbacks of remote user authentications

1. Detecting threats
2. New device, New threats
3. Network dependent

Two Factor Authentications

- Two factor authentication (2FA) is a security system that requires two distinct forms of identifications in order to access something
- The first factor is password and second commonly includes a text with a code sent to your phone, or biometrics using fingerprints, retinas, face etc

Types of 2FA

- Tokens
- Magnetic cards
- SMS OTP
- USB
- Mobile signatures

CHAPTER 5

Access Control: It is a data security process that enables organizations to manage who is authorized to access data and resources.

Mainly there are two types of access controls

Physical: It control limits access to computers,buildings rooms etc

Logical: It controls the limits of connections to computer network networks,system files, data etc

- Access Control gives the organization the ability to control restrict,monitor and protect resources
- It is the combination of authentication and authorizations

ACCESS Control principles

- **Authentication:** Verification that credentials of a user or other system entity is valid or not
- **Authorization:** The granting of a right permissions to a system entity to access a system resources.
  - Determines who is trusted for a given purpose
- **Audit:** An independent review and examination of system records and activities in order to test for adequacy of system controls.
  - Ensure compliance with established policy and operational procedures
  - Detect breaches in security
  - To recommend any indicated changes in control, policy and procedures

Subject, objects and access rights

Subjects: subject is a user or process run by a user. An entity capable of accessing the objects.Three classes are

- Owner: this may be creator of a resource, such as file
- Group: a named group of users may also be granted access rights.
- World: The least amount of access is granted to user who are able to access the system but are now included in the categories owner and group

Objects: it is the resources or data in system.

- A resources to which access is controlled.
- Entity contain and/or receive information
- e.g. records,blocks,pages,segments,files,directory etc

Subject, objects and access rights

Access right: Describes the way in which a subject may access objects

- Read: user may view information of system resources
- Write: user may add,modify data in system resources.
- Execute: user may execute specified program
- Delete: User may delete certain system resources such as files,resources etc
- Create: User may create new files,records or fields
- Search: user may list the files in a directory or otherwise search the directory

Access Control matrix (ACM)

- It is a table that defines access permissions between specified subjects and objects
- Rows of ACM corresponds to users/subjects/groups
- Columns corresponds to resources that need to be protected
- ACM [U,O] defines what access rights user U has for object O
- It is also called Lampson's access control matrix

Access Control Matrix

Object → / Domain ↓	File-1	File-2	File-3	File-4
D1	read write	read	read	read
D2	read	write	--	execute
D3	write	--	write	execute

Access Matrix

Access control lists (ACLs) and C-Lists

- ACL: Store lampson's access control matrix by column
- ACL are preferable when
  - Users manage their own files
  - Protection is data oriented

Capabilities or (C-lists)

- Store access control matrix by row
- With C-lists, it is easy to delegate (and sub-delegate and sub-sub-delegate and so on), and it is easier to add or delete users

ACL

Advantages of Access Control List:

- It is easy to change by removing the entry of the subject from the object's access control list.
- It is easy to review access by directly examining the access control list of objects.

Disadvantages of Access Control List:

- It imposes search overhead and results in poor efficiency as the entire access control list needs to be searched when access is made to an object.
- It requires more data storage space as data is stored object-wise and the same subject can have multiple access to multiple objects thereby consuming more storage space.

C-Lists

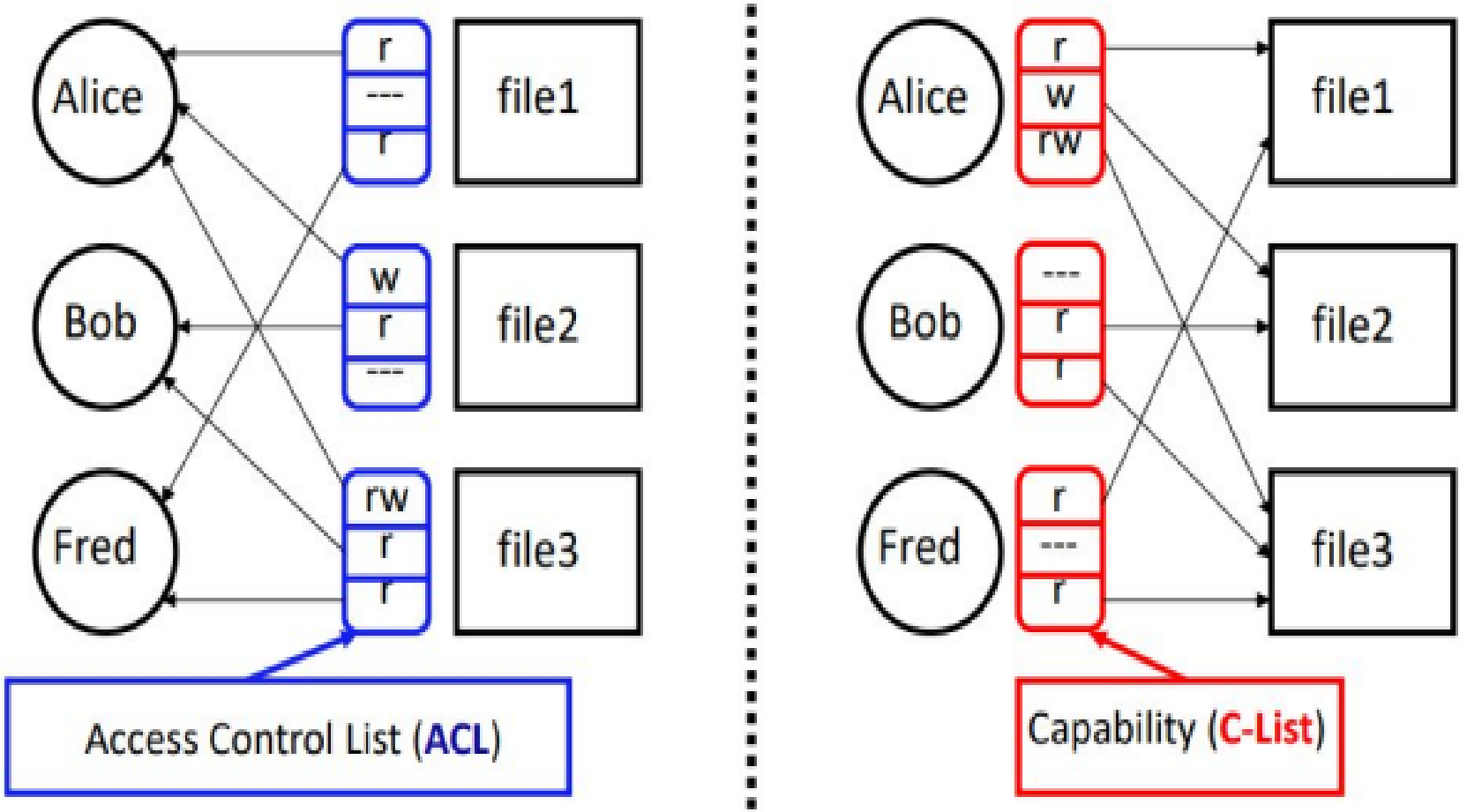
Advantages of Capability List:

- It is efficient as it frequently checks the validity of an address.
- It is flexible as users are allowed to define certain parameters.
- It is simple to understand as it allows natural correspondence between subjects and objects.

Limitations of Capability Lists:

- It is difficult to deallocate memory that is not currently in use.
- It is difficult to change access rights once assigned to subjects.
- It has complicated control of the propagation of various access rights.
- It is difficult to review the access provided to various subjects.

ACLs vs. Capabilities



- Note that arrows point in opposite directions...
- With ACLs, still need to associate users to files

Sr. No	Access Control Lists	Capability Lists
1.	It is defined object-wise (resources).	It is defined subject-wise (users, processes, and procedures).
2.	It lists the various subjects along with the rights of an object.	It lists the various objects along with the rights permitted on them for a subject.
3.	Each object (resource) has a list of pairs of the form <subject, access rights>	Each subject (user, process procedure) has a list of pairs of the form <object, access rights>
4.	It would be tedious to have separate listings for each object (user), therefore, they are grouped into classes. For example, in UNIX, there are three classes self, group, and anybody else.	Here capabilities are the names of the objects. The objects not referred to in at capability list cannot be ever named.
5.	The default is: Everyone should be able to access a file.	The default is: No one should be able to access a file unless they have been given a capability.
6.	Access lists are simple and are used in almost all file systems.	Capabilities are used in systems that need to be very secure as they prohibit sharing of information unless access is given to a subject.

Discretionary Access Control (DAC)

- Traditional method of implementing access control
- Scheme in which an entity may enable another entity to access some resources
- Often provided using an access matrix .
  - One dimension consist of identified subjects that may attempt data access to resources
  - The other dimension lists the objects that may be accessed
- Each entry in the matrix indicates the access rights of particular subject for particular objects

A general model for DAC

- **The model assumes**
  - A set of subjects
  - A set of objects
  - A set of rules that govern the access of subject to objects
- **Protection state:** Protection state of system to be the set of information, at a given point in time, that specifies the access rights for each subject with respect to each objects
- We can identify three requirements:
  - Representing the protection state.
  - Enforcing the access rights
  - And allowing subjects to alter the protection state in certain ways.

A gen

	file		
John	Owner		
Mary	Read, Write, Create		
Sue	Read	Read	Rea
Felix			Read, Write, Create
			Cre Delete

Role based Access Control (RBAC)

- Traditional DAC system defines the access rights of individual users and groups. RBAC is based on
  - Roles that user assume in a system (instead of their identity)
  - Role is a job function within an organization. A role will have specific access rights to one or more resources
  - Assign Access rights to Roles (instead of individual users)
  - Users assigned to different roles according to their responsibilities
  - User-to-Roles are Many-to-Many
- The set of users change frequently, and the assignment of user to one or many roles is also dynamic
- The set of rules is relatively static, with only occasional addition or deletion.
- The set of Resources and the specific access right associated with a particular role are also likely to change infrequently which is relatively static.

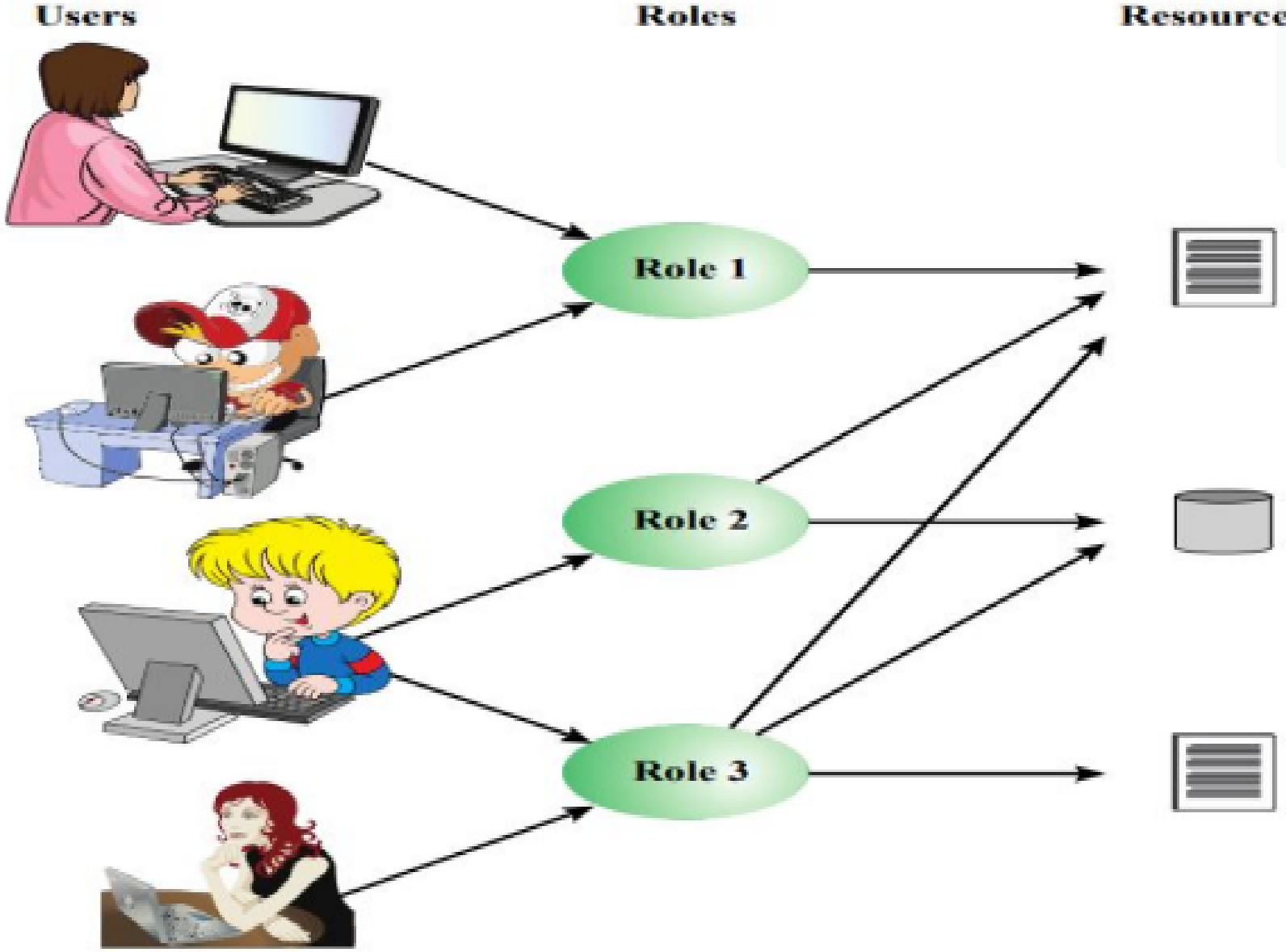
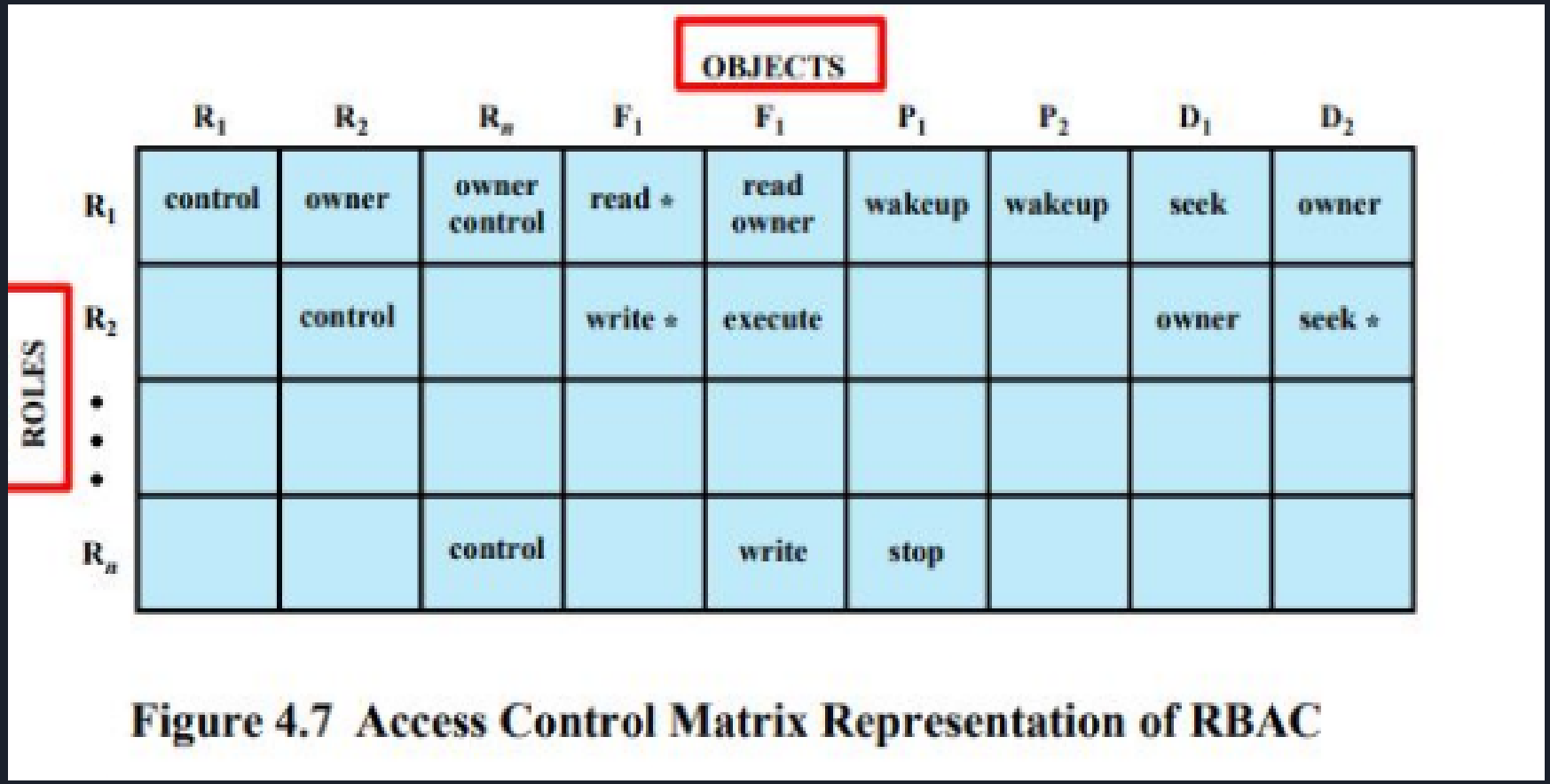


Figure 4.6 Users, Roles, and Resources

Best Practices of RBAC

- RBAC allows to
  - Segregate duties within teams
  - Grant only the amount of access to users that they need to perform the jobs
- Instead of giving everybody or group unrestricted permissions on a resources, you can allow only certain actions at a particular scope.
- Planning the access control strategy.
  - Each role should contain minimum set of access rights needed for that role.
  - Its a best practice to grant user the least privilege to get their work done

Access Control matrix of RBAC



ROLES	OBJECTS								
	R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
•									
•									
•									
R_n			control		write	stop			

Figure 4.7 Access Control Matrix Representation of RBAC

Roles

- A role contain the minimum set of access rights
- A user is assigned to a role that enables him/her to perform only what is required
- Multiple users may assigned to same role

A role assignment consist of three elements

- Security principal: object that represent a user,group and service principal
- Role definition: Collection of permissions
- Scope: set of resources that the access applies to

Limitation of RBAC

1. **Mutually Exclusive Roles:**
   - A user can only be assigned to one role in the set (either during session or statically)
   - Any permission (access right) can be granted to only one role in set
   - Separation of duties and capabilities (no collusion among individuals,roles have non-overlapping permissions)
2. **Cardinality:**
   - Setting a maximum number of users that can be assigned to a given role
   - The number of roles that a user is assigned to
   - The number of roles a user can be activate for a single session
3. **Prerequisite Roles:**
   - Dictates that a user can only assigned to a particular role if it is already assigned to some other specified role

Attribute Based Access Control (ABAC)

- Attribute based access control also known as policy-based access control (PBAC) or claim-based access control (CBAC), is an authorization methodology that sets and enforces policy based on characteristics, such as department,location, manager, and time of day.
- It uses Boolean logic with if-then statement statements that defines user, request,resources and action
- Example: if the requester is salesperson, they are granted read-write access to CRM solution as opposed to administrator who is only granted view privileges to create a report

Uses of ABAC

- Protecting data, network devices, cloud services and IT resources from unauthorized user or action
- Securing microservices / application programming interfaces (APIs) to prevent exposure of sensitive transactions
- Enabling dynamic network firewall controls by allowing policy decisions to be made on a per-user basis

Components of ABAC

- **Subject or user attributes:** It describes who is attempting to obtain access to a resources in order to perform an action. This includes username,age,job title,citizenship, user Id, security clearance etc . e.g LDAP, HR system
- **Object or resource attributes:** It includes characteristics of an object or resources (e.g. file,application,server,API) that has received a request for access. E.g creation date,last updated,author,owner,file name,file type and data sensitivity
- **Environmental or context attributes:** It indicates the broader context of access requests. Environmental attributes can be contextual items, such as time and location of an access attempt, the subject's device type, communication protocol, authentication strength, the subject's normal behavior patterns, the number of transactions, relationship with third party app etc

Components of ABAC

Action Attributes: This indicates how the user wants to engage with a resource. E.g view,read,write,copy,edit,transfer,delete etc

- These can be used individually or in combinations for more complex scenarios

Subject or User Attributes	Object or Resource Attributes	Environmental or Context Attributes	Action Attributes
Clearance	Author/Owner	Current Day	Delete
Department	Classification	Current Time	Read
Employee ID	Date Created	Device	Transfer
Job Title	Last Updated	Location	View
Username	Type	Time Zone	Write

HOW ABAC works

- An access request is made
- The attribute-based access control tool scans attributes to determine if they match existing policies
- Based on the result of ABAC tool's analysis, permissions is granted or denied
- Attributes are analyzed to accessed how they interact in an environment; then, rules are enforced based on relationship

Benefits of ABAC

- **Broad range of policies:** It allows situational variables to be controlled to help policy-makes implement granular access
- **Easy to use:** It is very user-intuitive. It hides technical permission sets behind an easy-to-use interface.
    - Anyone with right permissions can update a user profile and be assured that the user will have the access they need as long as their attributes are up to date.
    - The maximum number of users can be granted access to maximum available resources without administrator having to specify relationship between each user and objects

Benefits of ABAC

- **Fast onboarding of new users:** ABAC model expedite the onboarding of new staff and external partners by allowing administrators and object owner to create policies and assign attributes that give new users access to resources
    - With ABAC existing rules or object characteristics do not need to be changed to grant this access
- **Flexibility:** Almost any attribute can be represented and automatically changed based on contextual factors,such as application and types of data user can access, what transactions they can submit, and the operations they can perform
- **Scalability:** Once the ABAC has been setup, administrator can copy and reuse attributes for similar components and user positions, which simplifies policy maintenance and new user onboarding

Challenges of ABAC

- Implementation Complexity: this is because administrator must
  - Assign attributes to every components
  - Create a central policy engine to determine what attributes are allowed to do, based on various conditions
  - Define all attributes
  - Gauge the permissions available to specific users before all attributes and rules are in place
  - Map authorization policies to create comprehensive policy set to govern access

ABAC vs RBAC

ABAC	RBAC
Resources to support a complex implementation process	Need access controls, but lack resources for a complex implementation process
A large number of users with dynamic roles	Well-defined groups within the organization
Large organization with consistent growth	Organizational growth not expected to be substantial
Workforce that is geographically distributed	Workforce that is centrally located
Need for deep, specific access control capabilities	Comfortable with broad access control policies

Identity,Credentials and Access management

Identity, Credentials, and Access management (ICAM) is a set of security tools, policies, and systems that helps organizations manage,monitor, and secure access to their organizations, IT infrastructure.

- ICAM represent the combination of digital identities, credentials, and access control into a single comprehensive approach.
- ICAM reduces the risk of cyber attack to the organization by preventing unauthorized access to your network, system, and data

ICAM includes

- **Identity management:** Identifies a subject and establishes that they are who they claim to be when authorizing access to a system. (.i.e. Physical entity, digital entity)
- **Credential management:** Binds the identity of authenticator, allowing the system to identify the user through login (i.e. user authentication, identification card, username and password)
- **Access management:** Grants permissions for what users can do and see within a system (e.g. using specific groups and role for separation). Access management determines which roles or users can access different information and processes at specific times and levels of security (i.e. restrict access to a database unless the user is authenticated and is in a role that has been granted access to that resource).

Benefits of ICAM

- Improving your cyber security by limiting access to authorized users
- Simplifying your organization's user management
- Securing access to information
- Tracking access to sensitive information with more effective management
- Helping prevent identity fraud

Risks of ICAM

- Compromising sensitive information
- Spreading misinformation
- Compromising proper function of processes and equipment
- Damaging system and information integrity and availability
- Losing organization reputation and credibility
- Compromising execution of emergency processes
- Risking impacts to national security

Proper implementations of ICAM

- Password and passphrase
- Biometric
- MFA
- Principle of least privilege
- Cyber security training

Trust Frameworks

- Trust frameworks provide a common set of agreed upon standards for disparate entities to establish trust.
- Ensuring all organizations meet the same agreements and requirements allows for forgoing additional legal contracts and peer-to-peer agreements
- This is often referred as scalable trust, because each new connection between organizations and their user/clients grow the network rapidly in some cases
- Framework provides policy and technical interoperability for the issuers of digital identity credentials, the individual asserting their identities, and organizations relying on the identity assertions linked to digital credentials.

Components of Trust frameworks

- **Policies:** The common set of minimum requirements (policies) for network participants, identity providers, or users. The policies are published, allowing organizations that depend on those policies to conduct business to make a determination concerning trust.
- **Infrastructure:** The technical mechanisms of delivering a single source of truth of who/what is trusted
- **Certification:** The process of ensuring adherence to all Trust Framework requirements. DirectTrust federates trust by accrediting HISPs, Certificate Authorities, and Registration Authorities. Issuers within trust in identity environments are approved or revoked through regular audits and monitoring

Components of Trust frameworks

- **Interoperability:** The ability for information or credentials to be accepted and used easily and seamlessly by using a common set of standards
- **Technical Standards:** DirectTrust Standards develops standards and specifications that, when adopted, enable and promote healthcare interoperability using Direct exchange and/or trust frameworks.
- **Legality:** DirectTrust Standards develops standards and specifications that, when adopted, enable and promote healthcare interoperability using Direct exchange and/or trust frameworks.

Chapter 7

Network Security

Overview of network Security

Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft. It involves creating a secure infrastructure for devices, applications, users, and applications to work in a secure manner.

- Network Security refers to the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats.

Goals of network security

The primary goal of network security are confidentiality, integrity and availability

- **Confidentiality:** The function of confidentiality is to protect precious business data from unauthorized persons. Confidentiality part of network security makes sure that the data is available only to the intended and authorized persons
- **Integrity:** This goal means maintaining and assuring the accuracy and consistency of data. The function of integrity is to make sure that the data is reliable and is not changed by unauthorized persons.
- **Availability:** The function of availability in Network Security is to make sure that the data, network resources/services are continuously available to the legitimate users, whenever they require it

Working on network security

1. Physical Network Security: This is the most basic level that includes protecting the data and network through unauthorized personnel from acquiring control over the confidentiality of the network. These include external peripherals and routers that might be used for cable connections. The same can be achieved by using devices like biometric systems.

2. Technical Network Security: It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One is protected from unauthorized users, and the other is protected from malicious activities.

3. Administrative Network Security: This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.

Network protocol

1. TCP/IP protocol
2. DNS protocol
3. ICMP protocol

Email security MIME(multipurpose internet mail extension)

Email security is the practice of protecting email accounts and communications from unauthorized access, loss, or compromise.

- MIME is a standard in order to expand the limited capabilities of email.
- It is a supplementary protocol or a add on which allows non ascii data to be sent through email (using SMTP)
- It allows users to exchange different kinds of data files on internet like audio,video,images etc
- Email messages with MIME formatting are typically transmitted with standard protocols like SMTP,POP, IMAP
- It is also used in different protocols such as http, www etc

MIME Header

- **MIME version:** currently 1.0
- **Content-Type:** defines type of data used in message like audio,video etc
- **Content-Transfer-encoding:** tells method used for encoding
- **Content-Id:** helps in uniquely identifying the message
- **Content-description:** It depends weather the body is actually image,video,audio etc

Secure/MIME (S/MIME)

- Secure / multipurpose internet mail extension
- Provides security by encrypting mails.
- It is widely accepted protocol for sending digitally signed and encrypted message i.e. It allows us to digitally sign our email to verify ourselves as the legitimate senders and also encryption and decryption of emails.
- S/MIME is based on asymmetric key encryption.

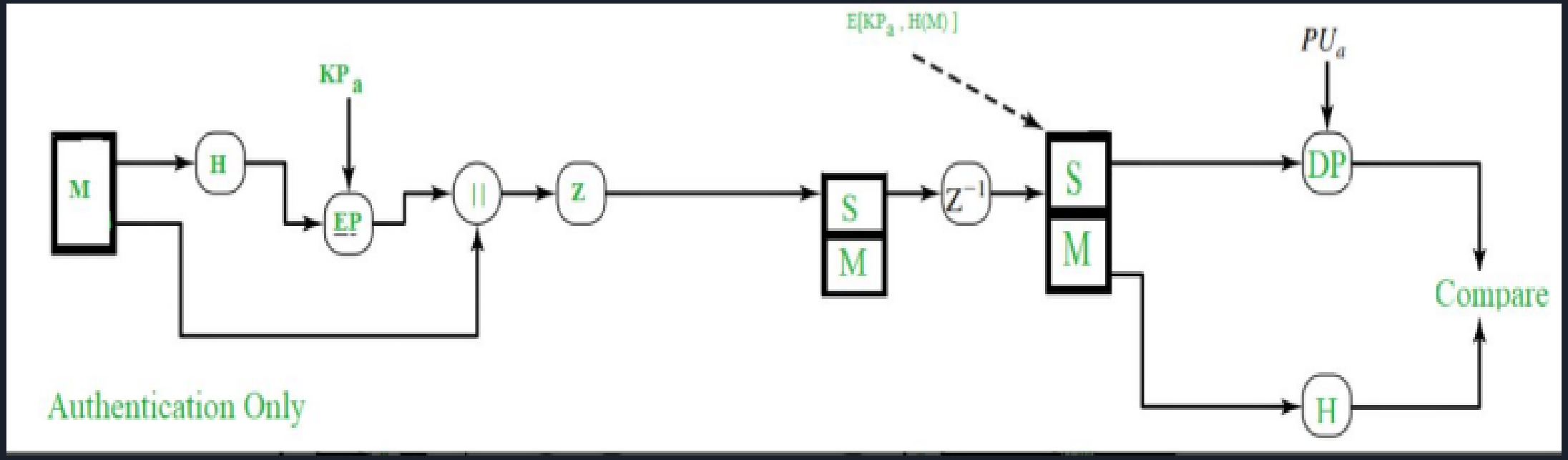
S/MIME properties

1. Authentication
2. Message integrity
3. Non-repudiation of origin (using digital signatures)
4. Privacy
5. Data security (using encryptions)

Pretty Good policy (PGP)

- It is an encryption program that provides cryptographic privacy and authentication for data communication
- Increases security of email communication via providing the cryptographic privacy and authentication
- PGP is used for signing,encrypting, and decrypting texts,emails,files,directories, and to increase security of email communications
- It helps on authentication (using digital signature) and confidentiality

Working of PGP -> Authentication only



Working of PGP -> Authentication only

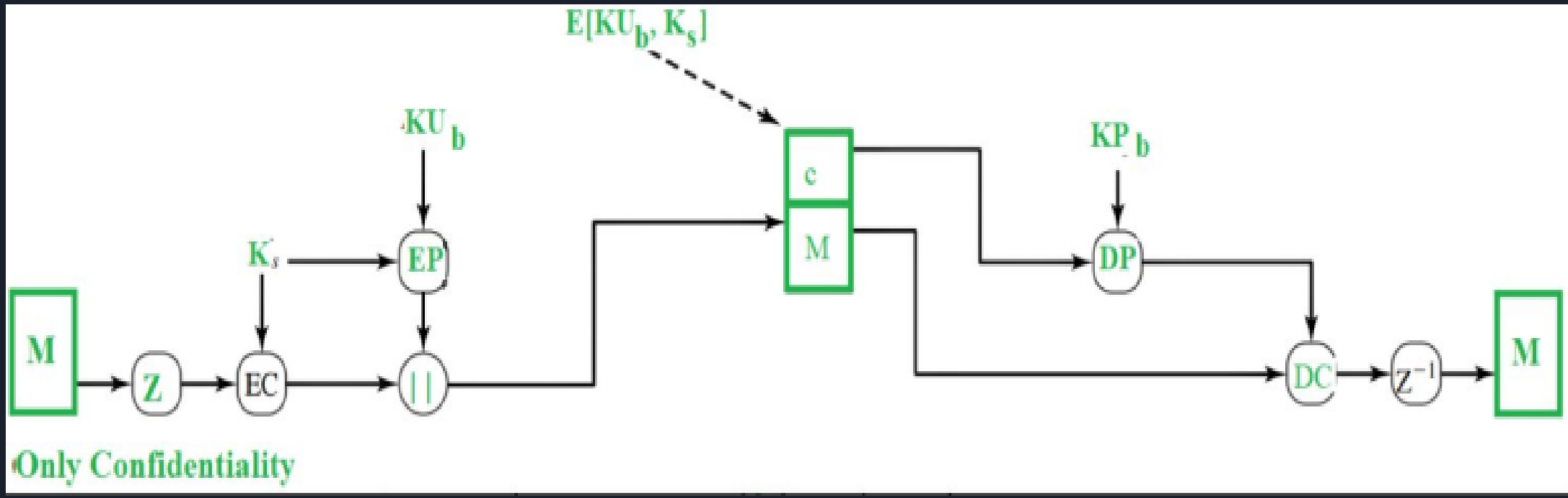
At Sender Side

- Hash function (H) calculates the hash value of message (M)
- Then using sender private key (KPa), it is encrypted called as digital signature
- The message is then appended to a signature
- The message is then compressed to reduce transmission overhead and is sent it to receiver

At Receiver Side

- The data is decompressed and the message and signature are obtained
- The signature is decrypted using sender public's key (PUa) and hash value is obtained
- The message is again passed to has function and its hash value is calculated and obtained
- Both value one from signature and other from output of hash function are compared and if both are same, email is sent from legit else it means the email has been compromised

Working of PGP -> Confidentiality only



Working of PGP -> Confidentiality only

At Sender

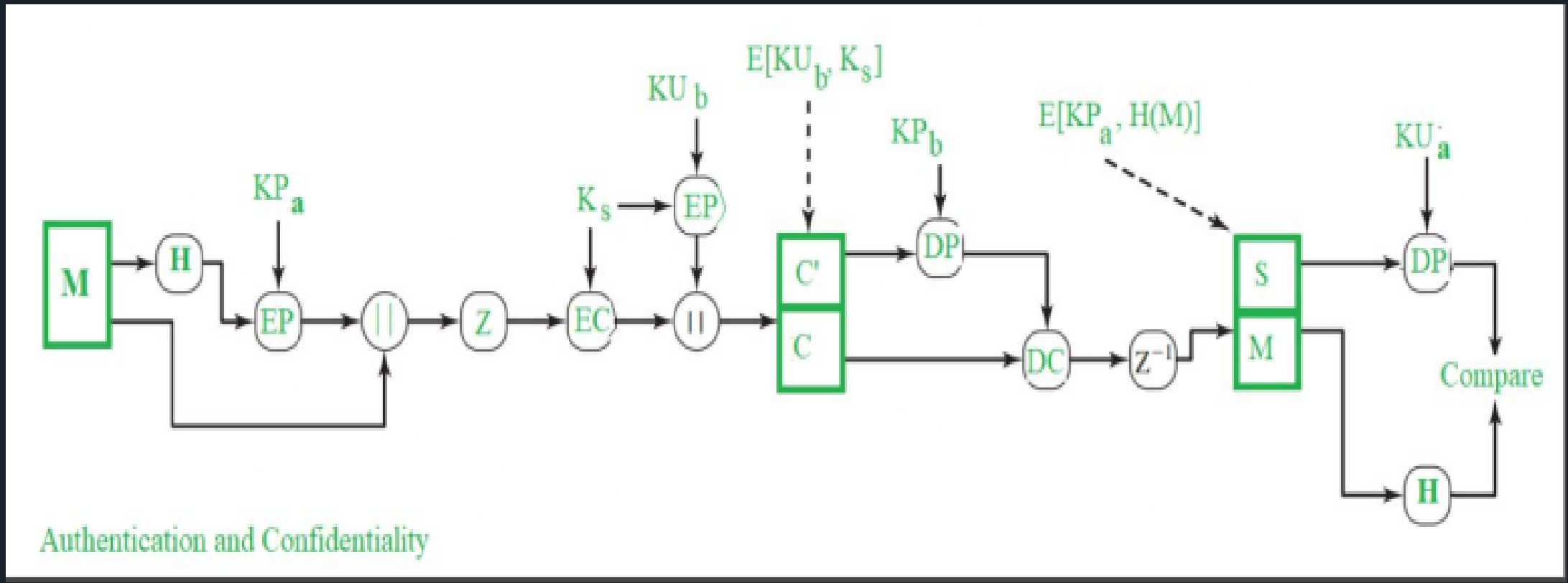
- The message is first compressed
- 128 bit session key (Ks) is used to encrypt the message through symmetric encryption
- Then symmetric key (Ks) itself gets encrypted through public key (EP) using the receiver public key (KUb)
- Both encrypted entities are now concatenated and sent to receiver

Working of PGP -> Confidentiality only

At receiver

- The encrypted session key is decrypted using receiver private key (KPb)
- The message is decrypted using obtained session key
- Then the message is decompressed to get the original message

Working of PGP Authentication and confidentiality



Note:

M – Message

H – Hash Function

K_s – A random Session Key created for Symmetric Encryption purpose

DP – Public-Key Decryption Algorithm

EP – Public-Key Encryption Algorithm

DC – Asymmetric Decryption Algorithm

EC – Symmetric Encryption Algorithm

KP_b – A private key of user B used in Public-key encryption process

KP_a – A private key of user A used in Public-key encryption process

PU_a – A public key of user A used in Public-key encryption process

PU_b – A public key of user B used in Public-key encryption process

|| – Concatenation

Z – Compression Function

Z^{-1} – Decompression Function

SSL and TLS

Secure sockets layer (SSL) is a standard technique for transmitting documents across a network.

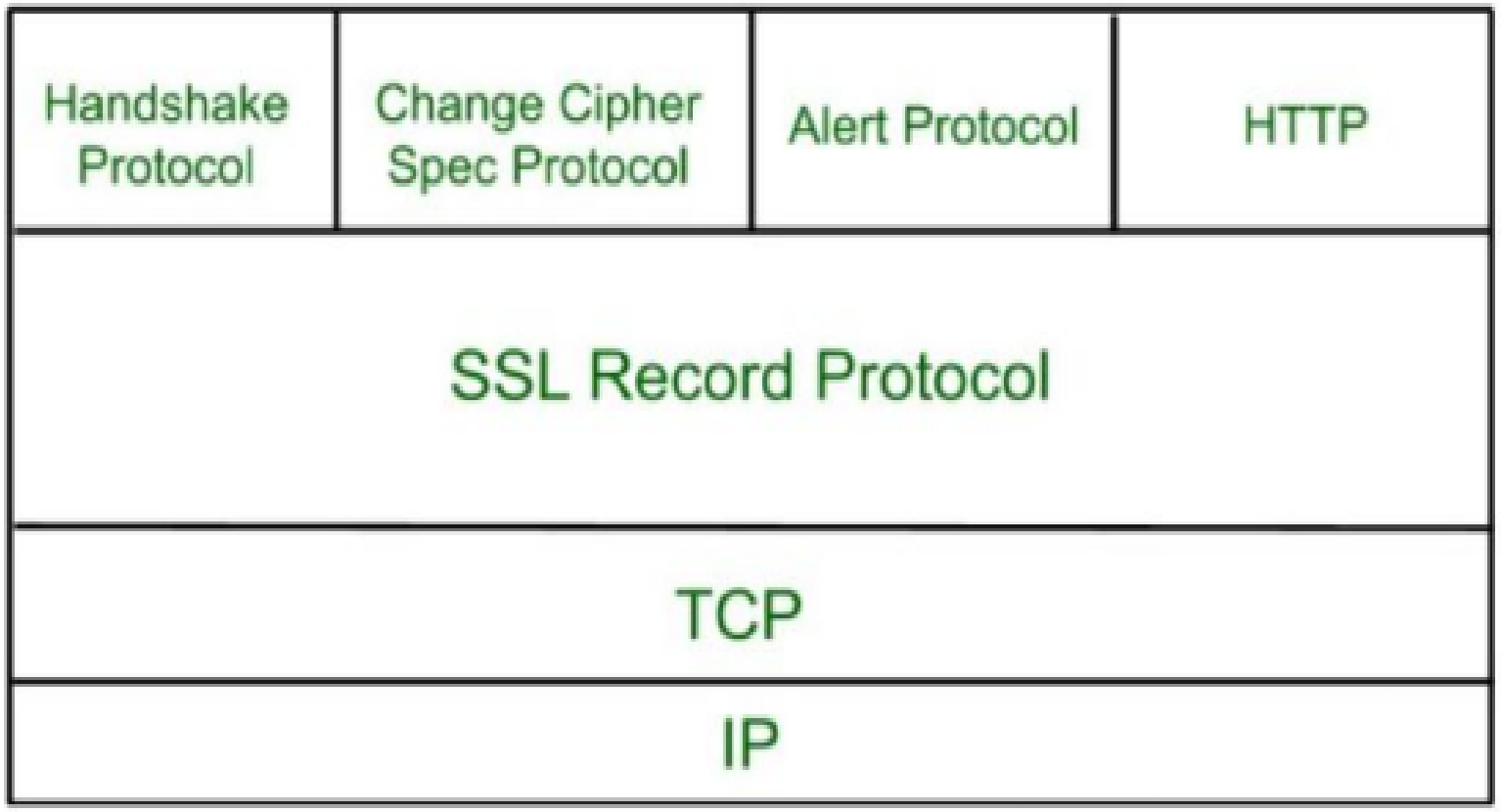
- A Web server requires an SSL certificate to establish a secure SSL connection while using SSL for safe Internet transactions. SSL encrypts network connection segments atop the transport layer, a network connection component above the program layer

The goals of SSL are as follows

- **Data integrity:** Information is safe from tampering. The SSL Record Protocol, SSL Handshake Protocol, SSL Change Cipher Protocol, and SSL Alert Protocol maintain data privacy
- **Client-server authentication:** The SSL protocol authenticates the client and server using standard cryptographic procedures.
- SSL is the forerunner of Transport Layer Security (TLS), a cryptographic technology for secure data transfer over the Internet.

SSL Headers/protocols

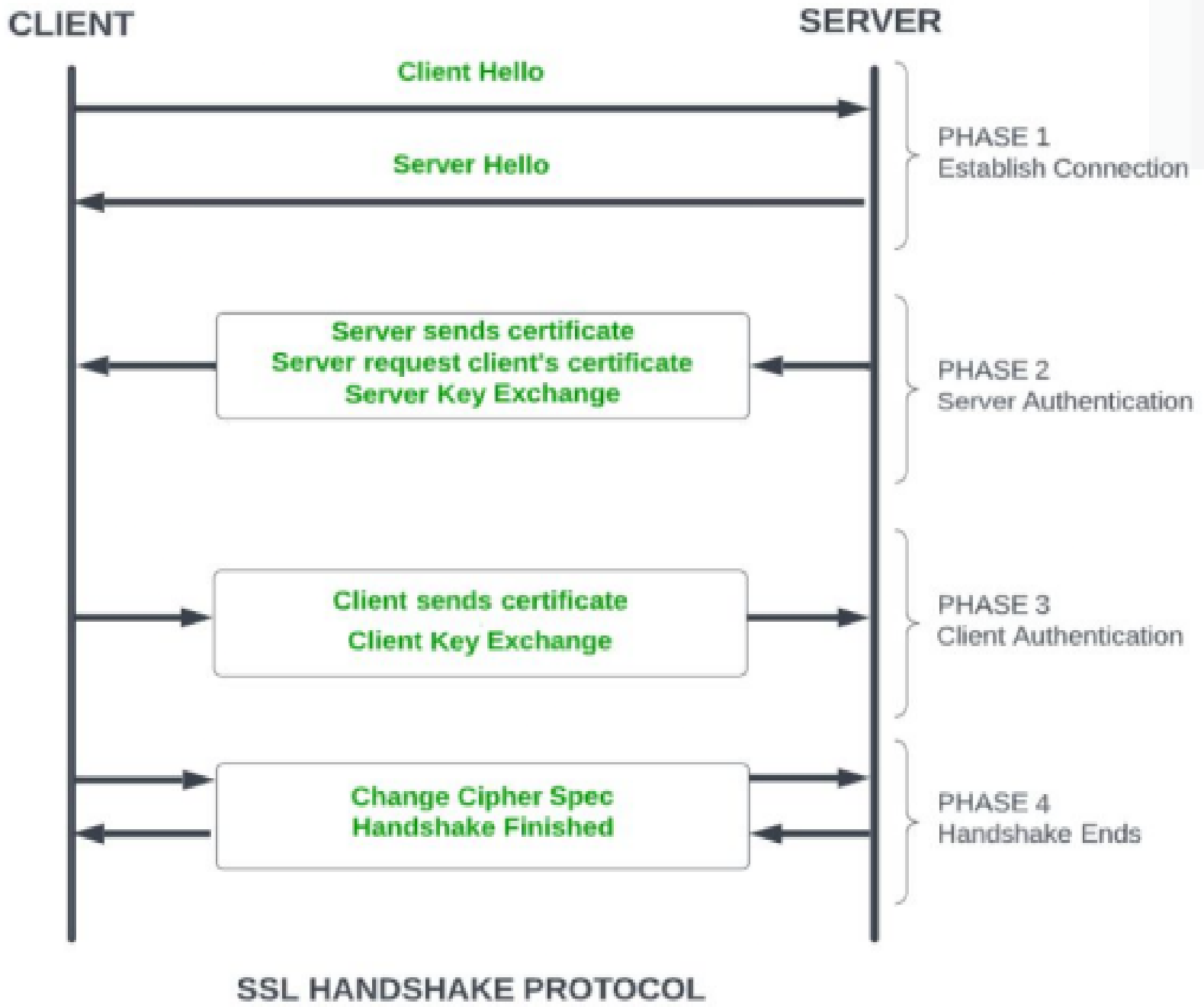
SSL Protocol Stack:



SSL protocol

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

- **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
- **Phase-2:** Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- **Phase-3:** In this phase, Client replies to the server by sending his certificate and Client-exchange-key.
- **Phase-4:** In Phase-4 Change-cipher suite occurs and after this the Handshake Protocol ends.



SSL Handshake Protocol Phases diagrammatic representation

Change-Cipher protocol

This protocol uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state. After the handshake protocol, the Pending state is converted into the current state.

- Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol's purpose is to cause the pending state to be copied into the current state.

Alert Protocol

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.

Level 1 Error: Warning Level

- **Bad certificate:** When the received certificate is corrupt.
- **No certificate:** When an appropriate certificate is not available.
- **Certificate expired:** When a certificate has expired.
- **Certificate unknown:** When some other unspecified issue arose in processing the certificate, rendering it unacceptable.
  Close notify: It notifies that the sender will no longer send any messages in the connection.
- **Unsupported certificate:** The type of certificate received is not supported.
- **Certificate revoked:** The certificate received is in revocation list.

Alert Protocol

Level 2(Fatal Error):

- **Handshake failure:** When the sender is unable to negotiate an acceptable set of security parameters given the options available.
- **Decompression failure**: When the decompression function receives improper input.
- **Illegal parameters:** When a field is out of range or inconsistent with other fields.
- **Bad record MAC:** When an incorrect MAC was received.
- **Unexpected message:** When an inappropriate message is received

This alert breaks the connection between sender and receiver. The connection will be stopped, cannot be restarted.

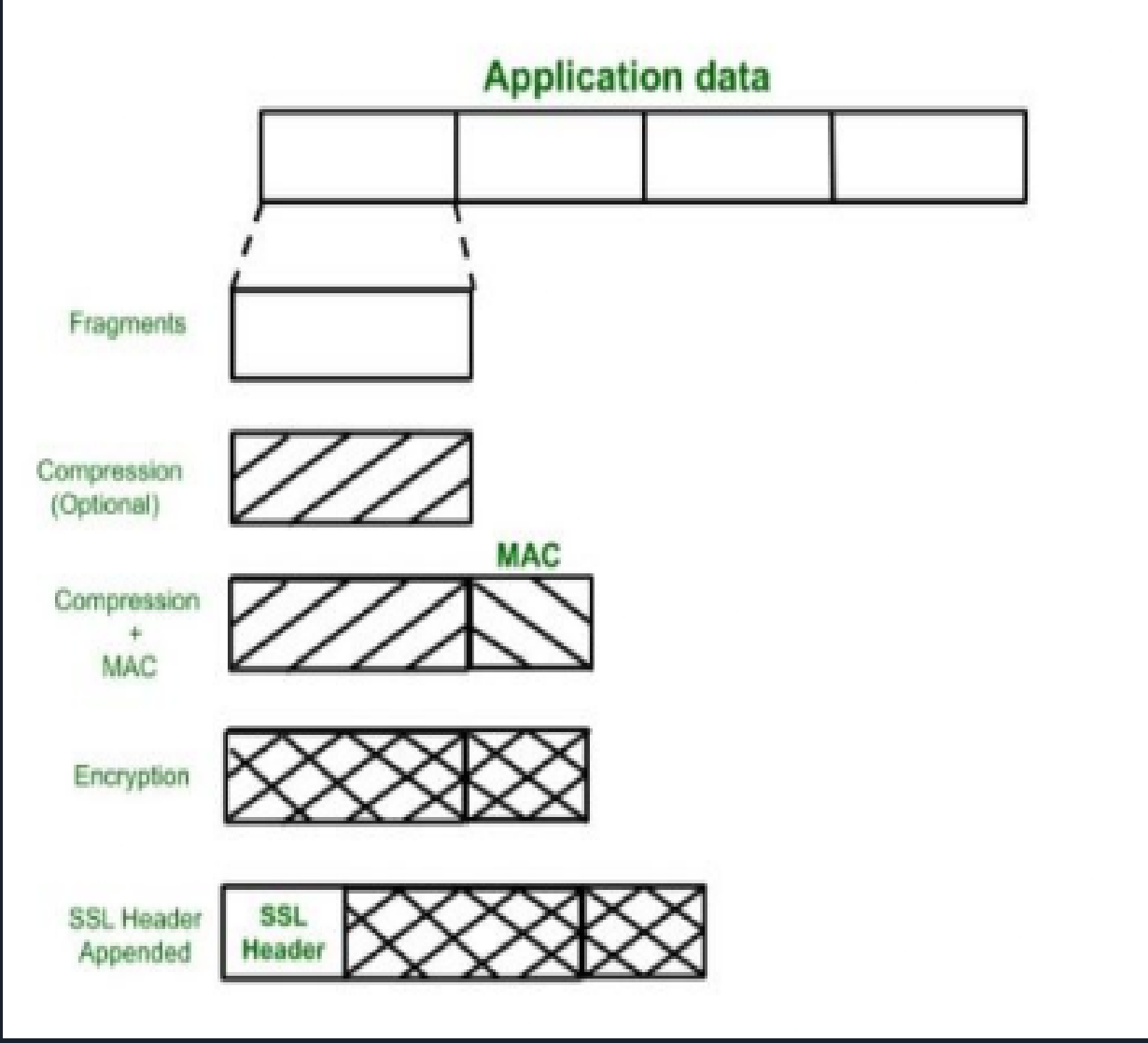
SSL Record protocol

SSL Record provides two services to SSL connection

- Confidentiality
- Message integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.

SSL Record protocol



Characteristics of SSL

- Encryption
- Authentication
- Integrity
- Non-repudiation
- Public-key cryptography
- Session management
- Certificate issued by trusted CA

Transport layer security (TLS)

Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called SSL. TLS ensures that no third party may eavesdrop or tampers with any message.

- **Encryption:**

  TLS/SSL can help to secure transmitted data using encryption.

- **Interoperability:**

  TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.

Transport layer security (TLS)

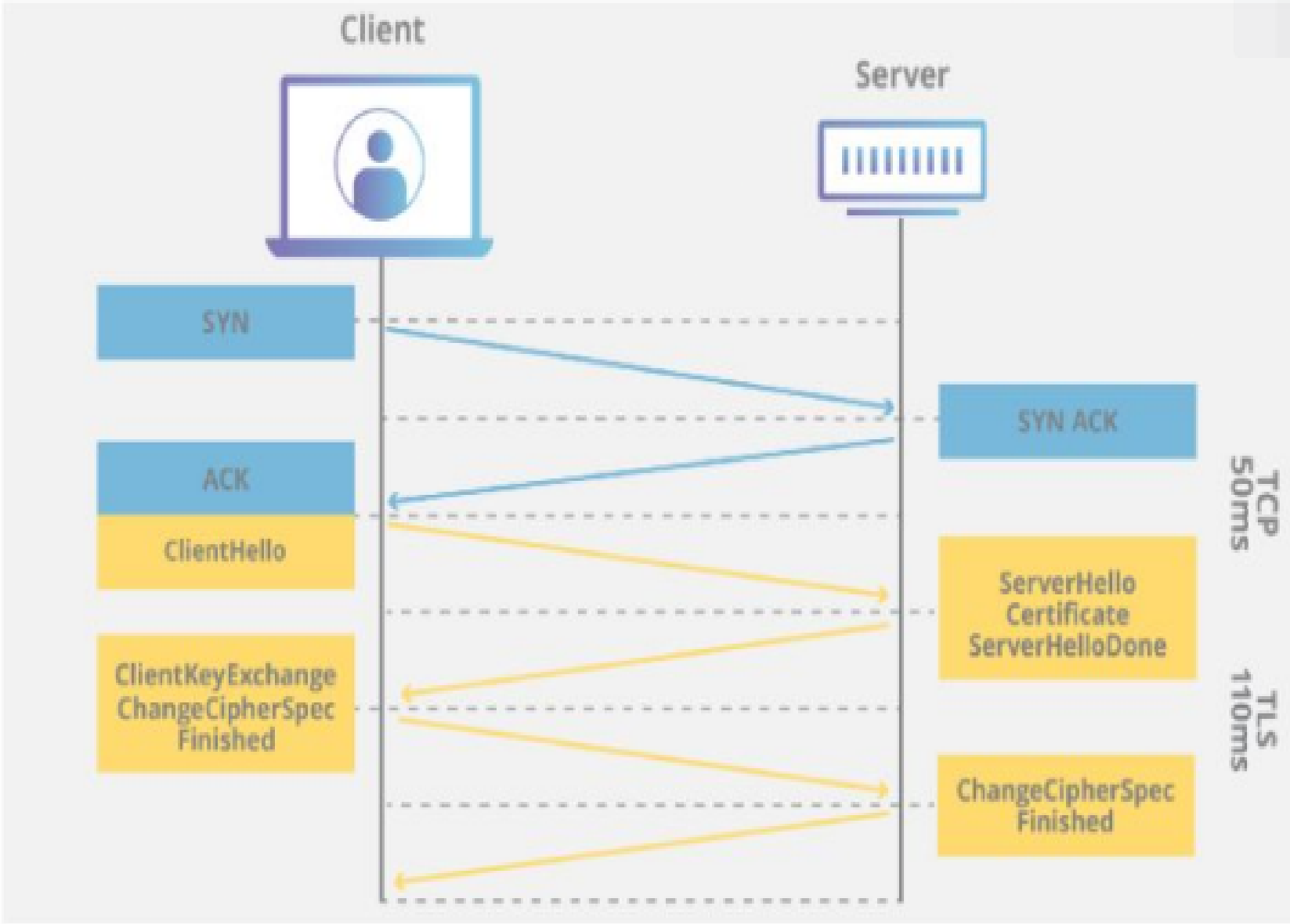
- **Algorithm flexibility:**
  TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment:**
  Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
- **Ease of Use:**
  Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client

Working of TLS

The client connects to server (using TCP), the client will be something. The client sends number of specifications:

1. Version of SSL/TLS
2. Which cipher suites, compression methods it wants to use

- The server checks what the highest SSL/TLS version that is supported by both of them, picks a cipher suite from client
- After this basic setup, the server provides its certificate.
- This certificate must be trusted by the client itself of the party that the client trusts.
- After verification of server (that the server is actually server not the Man in the middle), a key is exchanged.
- This key can be public key, "preMasterSecret" or simply blank depending upon the cipher suite.
- Both the server and client now compute the key for symmetric encryption.
- The handshake is finished and two hosts can communicate securely



Pros of TLS

- Preventing eavesdropping and tampering
- Providing data integrity
- Improving SEO
- Enhancing customer trust
- Offering granular control

SSL	TLS
SSL stands for Secure Socket Layer.	TLS stands for Transport Layer Security.
SSL (Secure Socket Layer) supports the **Fortezza** algorithm.	TLS (Transport Layer Security) does not support the **Fortezza** algorithm.
SSL (Secure Socket Layer) is the 3.0 version.	TLS (Transport Layer Security) is the 1.0 version.
In SSL(Secure Socket Layer), the Message digest is used to create a master secret.	In TLS(Transport Layer Security), a Pseudo-random function is used to create a master secret.
In SSL(Secure Socket Layer), the Message Authentication Code protocol is used.	In TLS(Transport Layer Security), Hashed Message Authentication Code protocol is used.
SSL (Secure Socket Layer) is more complex than TLS(Transport Layer Security).	TLS (Transport Layer Security) is simple.
SSL (Secure Socket Layer) is less secured as compared to TLS(Transport Layer Security).	TLS (Transport Layer Security) provides high security.
SSL is less reliable and slower.	TLS is highly reliable and upgraded. It provides less latency.
SSL has been depreciated.	TLS is still widely used.
SSL uses port to set up explicit connection.	TLS uses protocol to set up implicit connection.

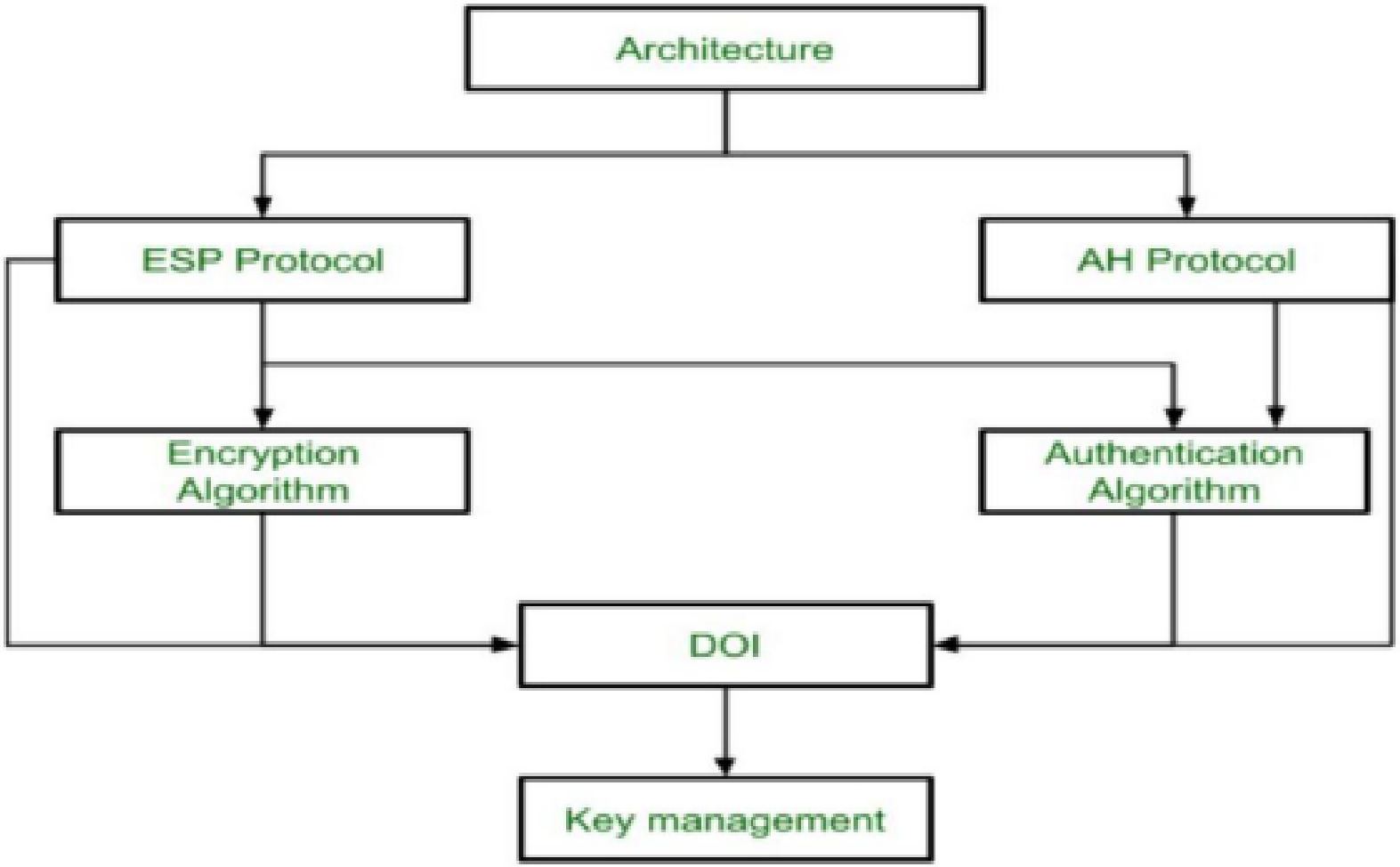
IP security

IP Sec (Internet Protocol Security) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted, and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Components of IPSec

1. Encapsulating Security Payload (ESP)
2. Authentication Header (AH)
3. Internet Key Exchange (IKE)

Architecture of IP Security



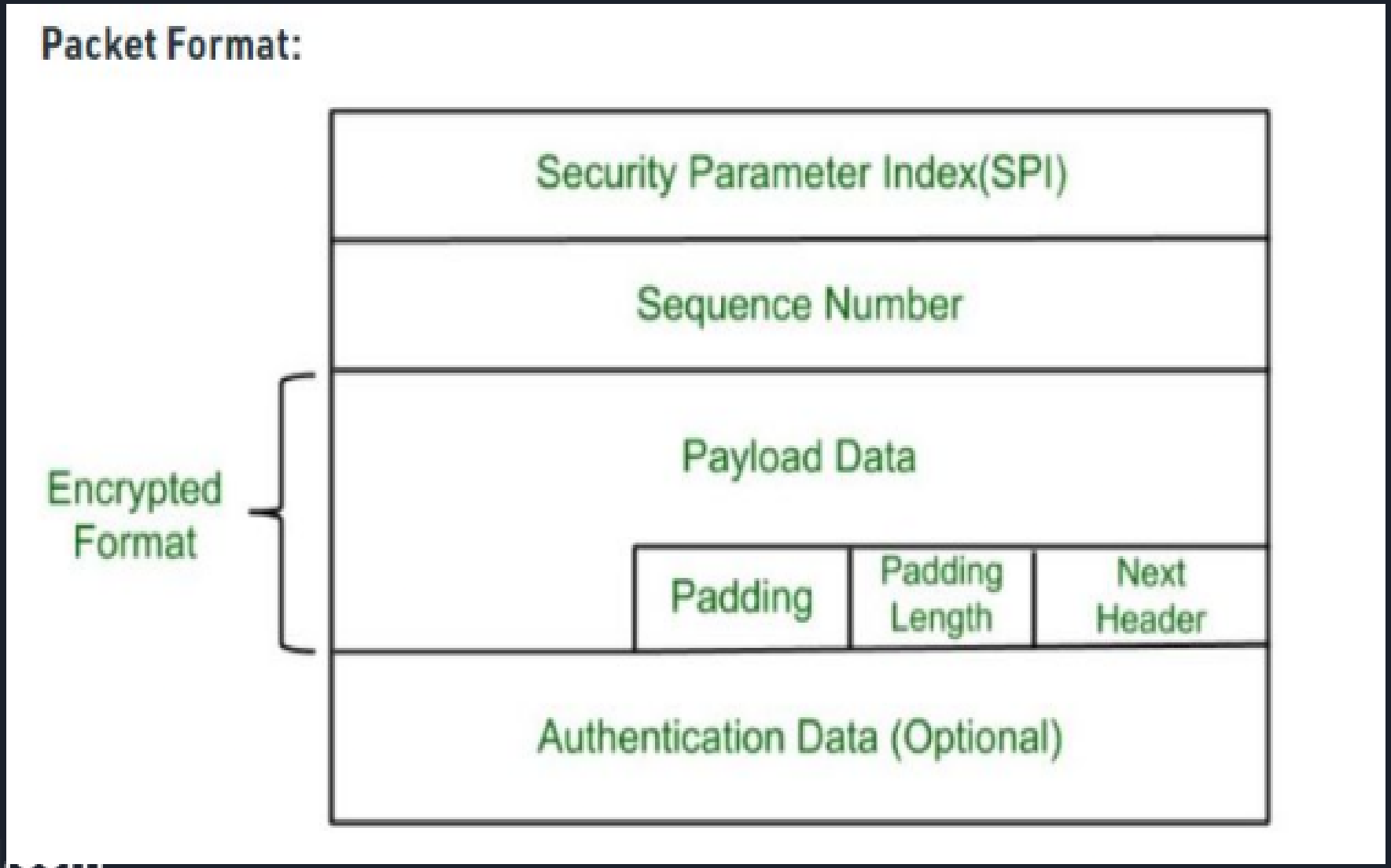
IP Security Architecture

Architecture of IPSec

- Architecture: Architecture or IPSec architecture covers the general concepts, definition, protocols, algorithm and security requirements of IP Security technology

- ESP Protocol: ESP (Encapsulation security Payload) provides a confidentiality service. Encapsulation payload is implemented in either two ways
  - ESP with optional Authentication
  - ESP with Authentication

ESP Packet format



ESP

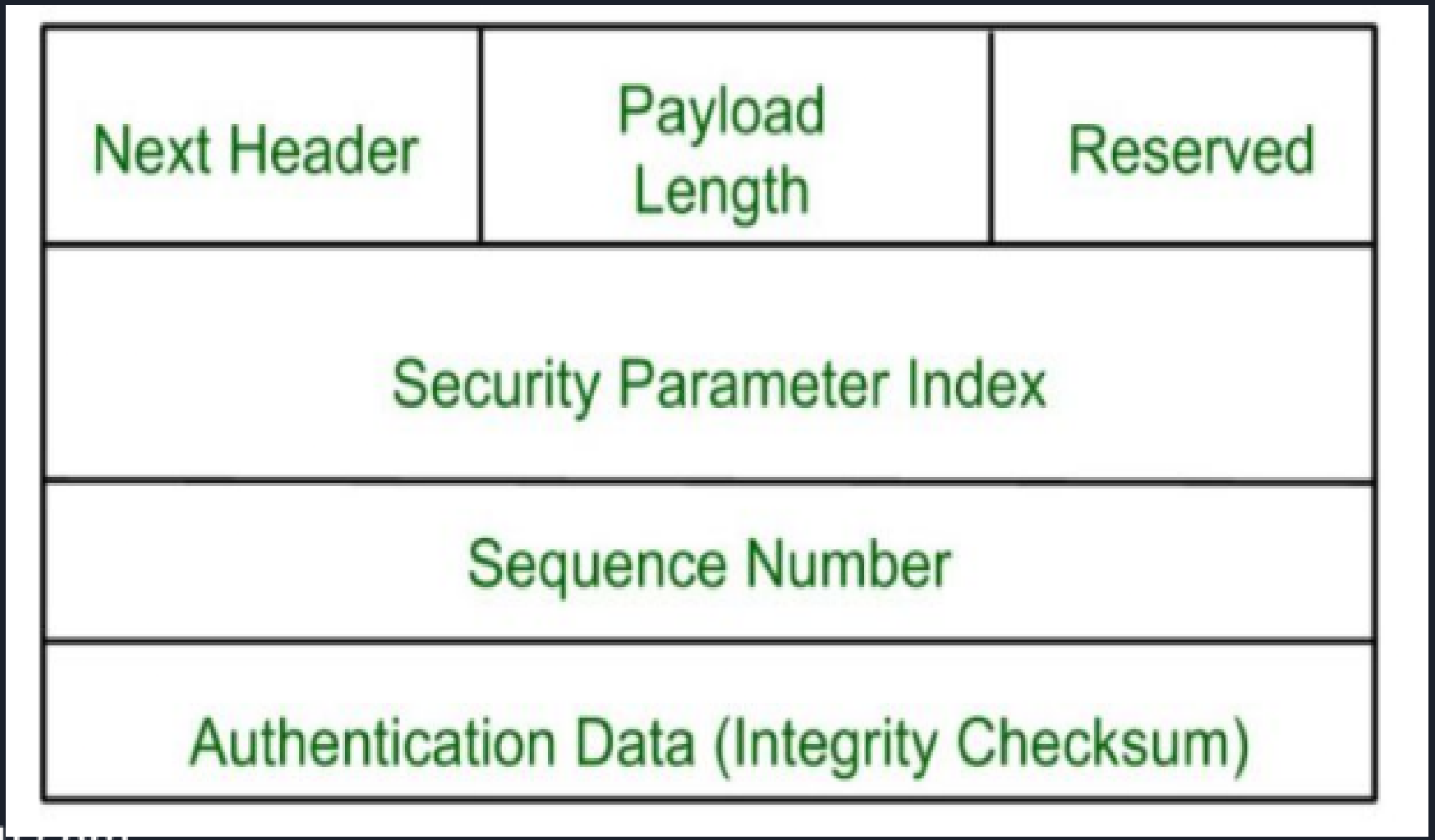
- **Security Parameter Index(SPI):** This parameter is used by security Association. It is used to give a unique number to the connection built between client and Server
- **Sequence number:** unique sequence numbers are allotted to every packet so that on the receiver side packets can be arranged properly
- **Payload data:** payload data means the actual data or the actual message. The payload data is in an encrypted format to achieve confidentiality
- **Padding:** Extra bits of space are added to the original message in order to ensure confidentiality. Padding length is the size of the added bits of space in the original message
- **Next Header:** Next header means the next payload or next actual message
- **Authentication Data:** This field is optional in ESP protocol packet format

IPSec Architecture

- **Encryption algorithm:** The encryption algorithm is the document that describes various encryption algorithms used for Encapsulation security payload

- **AH Protocol:** AH (Authentication Header) protocol provides both Authentication and integrity service. Authentication header is implemented only with integrity
    - Authentication header covers the packet format and general issue related to the use of AH for packet authentication and integrity

Authorization Header (AH)



Authentication Header

- **Next Header:** It is a 8-bit field that identifies type of header present after authentication header
- **Payload Length:** The length of the payload that we are sending
- **Reserved:** this is 16-bit field which is reserved for future use
- **Security parameter Index (SPI):** It is very important field which identifies all packets which belongs to present connection. If we're sending data from Source A to Destination B. Both A and B will already know algorithm and key they are going to use. So for Authentication, hashing function and key will be required which only source and destination will know about. Secret key between A and B is exchanged by method of Diffie Hellman algorithm. So Hashing algorithm and secret key for Security parameter index of connection will be fixed. Before data transfer starts security association needs to be established. In **Security Association**, both parties needs to communicate prior to data exchange. Security association tells what is security parameter index, hashing algorithm and secret key that are being used.

Authentication Header

- **Sequence Number:** This unsigned 32-bit field contains counter value that increases by one for each packet sent. Every packet will need sequence number. It will start from 0 and will go till 2^32 – 1.
- **Authentication Data (Integrity Check Value):** Authentication data is variable length field that contains Integrity Check Value (ICV) for packet. Using hashing algorithm and secret key, sender will create message digest which will be sent to receiver. Receiver on other hand will use same hashing algorithm and secret key. If both message digest matches then receiver will accept data. Otherwise, receiver will discard it by saying that message has been modified in between. So basically, authentication data is used to verify integrity of transmission.

IPSec Architecture

- **Authentication Algorithm:** The authentication algorithm contains set of documents that describes authentication algorithm used for AH and for the authentication option of ESP
- **DOI (Domain of Interpretation):** DOI is the identifier that supports both AH and ESP protocols. It contains value needed for documentation related to each other
- **Key Management:** Key management contains the document that describes how the keys are exchanged between sender and receiver

IP security

Internet Key Exchange (IKE): It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices.

- The protocol ensures security for VPN negotiation, remote host and network access
- The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication.
- The algorithm's IPSec users produce a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets that are not authorized are discarded and not given to the receiver.

The Key Management Protocol (ISAKMP) and Internet Security Association provides a framework for authentication and key exchange. ISAKMP tells how the setup of the Security Associations (SAs) and how direct connections between two hosts are using IPsec. Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5.

IP Security Architecture

IpSec uses two protocols to secure the traffic or data flow. These protocol are ESP (Encapsulation security payload) and AH (Authentication Header). IpSec Architecture includes protocol,algorithms,DOI, and key management. These component are important in order to provide three main services :

- Confidentiality
- Authenticity
- Integrity

Working on IPSec

- The hosts checks if packets should be transmitted using IPsec or not.This packet traffic triggers the security policy for itself. This is done when system sending the packet applies appropriate encryption. The incoming packets are also checked by host that they are encrypted properly or not
- Then IKE Phase 1 starts in which the 2 hosts (using IPSec) authenticate themselves to each other to start a secure channel. It has two modes. The Main mode provides greater security and Aggressive mode which enables the host to establish an IPSec circuit more quickly
- The channel created in last step is then used to securely negotiate the way IP circuit will encrypt data across the IP circuit
- Now, the IKE Phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithm to use on the session and agree on secret keying material to be used with those algorithm

Working on IPSec

- Then the data is exchanged across the newly created IPSec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPSec SAs
- When the communication between the host is completed or the session times out then the IPSec tunnel is terminated by discarding the keys by both the host

Features of IPSec

1. **Authentication:** IPSec provides authentication of IP packets using digital signatures or shared secrets. This helps ensure that the packets are not tampered with or forged.
2. **Confidentiality:** IPSec provides confidentiality by encrypting IP packets, preventing eavesdropping on the network traffic.
3. **Integrity:** IPSec provides integrity by ensuring that IP packets have not been modified or corrupted during transmission.
4. **Key management:** IPSec provides key management services, including key exchange and key revocation, to ensure that cryptographic keys are securely managed.
5. **Tunneling:** IPSec supports tunneling, allowing IP packets to be encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or L2TP (Layer 2 Tunneling Protocol).
6. **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
7. **Interoperability:** IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments.

Advantage of IPSec

1. **Strong security:** IPSec provides strong cryptographic security services that help protect sensitive data and ensure network privacy and integrity.
2. **Wide compatibility:** IPSec is an open standard protocol that is widely supported by vendors and can be used in heterogeneous environments.
3. **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
4. **Scalability:** IPSec can be used to secure large-scale networks and can be scaled up or down as needed.
5. **Improved network performance:** IPSec can help improve network performance by reducing network congestion and improving network efficiency.

Disadvantages of IPSec

1. **Configuration complexity:** IPSec can be complex to configure and requires specialized knowledge and skills.
2. **Compatibility issues:** IPSec can have compatibility issues with some network devices and applications, which can lead to interoperability problems.
3. **Performance impact:** IPSec can impact network performance due to the overhead of encryption and decryption of IP packets.
4. **Key management:** IPSec requires effective key management to ensure the security of the cryptographic keys used for encryption and authentication.
5. **Limited protection:** IPSec only provides protection for IP traffic, and other protocols such as ICMP, DNS, and routing protocols may still be vulnerable to attacks.

Firewall and their type

- A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

Types of firewall

1. Packet filtering firewall:
   - They compare each packet received to a set of established criteria, such as the allowed IP addresses, packet type, port number and other aspects of the packet protocol headers.
   - Packets that are flagged as troublesome are dropped -- that is, they are not forwarded and, thus, cease to exist.

Advantage of Packet filtering firewall

- A single device can filter traffic for the entire network
- Extremely fast and efficient in scanning traffic
- Inexpensive
- Minimal effect on other resources, network performance and end-user experience

Disadvantage of Packet filtering firewall

- Because traffic filtering is based entirely on IP address or port information, packet filtering lacks broader context that informs other types of firewalls
- Doesn't check the payload and can be easily spoofed
- Not an ideal option for every network
- Access control can be difficult to set up and manage

Firewall Types

2. Circuit-level gateway:

- It monitors TCP handshakes and other network protocol session initiation message across the network as they are established between the local and remote hosts to determine whether the session being initiated is legitimate
- They do not inspect packet themselves

Advantages:

- Only processes requested transactions; all other traffic is rejected
- Easy to set up and manage
- Low cost and minimal impact on end-user experience

Circuit-level gateway

Disadvantages:

- If they aren't used in conjunction with other security technology, circuit-level gateways offer no protection against data leakage from devices within the firewall
- No application layer monitoring
- Requires ongoing updates to keep rules current

Firewall Types

3. Application-level gateway:

- It is also referred as proxy firewall
- It functions as the only entry point to and exit point from the network
- It filters packet not only according to services for which they are intended, but also other characteristics such as HTTP request strings

Advantages:

- Examines all communications between outside sources and devices behind the firewall, checking not just address, port and TCP header information, but the content itself before it lets any traffic pass through the proxy
- Provides fine-grained security controls that can, for example, allow access to a website but restrict which pages on that site the user can open

Application-level gateway

Disadvantages:

- Can inhibit network performance
- Costlier than some other firewall options
- Requires a high degree of effort to derive the maximum benefit from the gateway
- Doesn't work with all network protocol

Firewall Types

4. Stateful inspection Firewall:

- It not only examines each packets but also keep track of whether or not packet is a part of established TCP or other network sessions.
- This offers more security than either packer filtering or circuit monitoring alone.

Advantages:

- Monitors the entire session for the state of the connection, while also checking IP addresses and payloads for more thorough security
- Offers a high degree of control over what content is let in or out of the network
- Does not need to open numerous ports to allow traffic in or out
- Delivers substantive logging capabilities

Stateful inspection firewall

Disadvantages:

- Resource-intensive and interferes with the speed of network communications
- More expensive than other firewall options
- Doesn't provide authentication capabilities to validate traffic sources aren't spoofed

Firewall Types:

5. Next-generation Firewall (NGFW):

- A typical NGFW combines packet inspection with stateful inspection and also includes some variety of deep packet inspection as well as other network security systems, such as IDS,IPS, malware filtering and antivirus

Advantages:

- Combines DPI (Deep packet inspection) with malware filtering and other controls to provide an optimal level of filtering
- Tracks all traffic from Layer 2 to the application layer for more accurate insights than other methods
- Can be automatically updated to provide current context

Next generation firewall

Disadvantages:

- In order to derive the biggest benefit, organizations need to integrate NGFWs with other security systems, which can be a complex process
- Costlier than other firewall types

Chapter 8

Security Audit

Security Audit

- An IT security audit is a comprehensive assessment of an organization's security posture and IT infrastructure. Conducting an IT security audit helps organizations find and assess the vulnerabilities existing within their IT networks, connected devices, and applications. It gives you the opportunity to fix security loopholes and achieve compliance.
- It is a form of auditing that focuses on security of an organization's information system assets.

Importance of IT security audit

- Protects the critical data resources of an organization.
- Keeps the organization compliant to various security certifications.
- Identifies security loopholes before the hackers.
- Keeps the organization updated with security measures.
- Identifies physical security vulnerabilities.
- Helps in formulating new security policies for the organization.
- Prepares the organization for emergency response in case of a cybersecurity breach.

Security Auditing architecture

- **Security protocols:** A security architecture defines in detail the tools and processes used in threat detection and prevention, as well as those used in incident response (the set of instructions that guides IT professionals in dealing with security breaches) and disaster recovery (a detailed plan that allows business processes to resume or continue despite a security incident). For instance, the security architecture might include specific requirements that security software vendors need to fulfill to win a bid. Incident response refers to

Security Auditing architecture

- **Account creation and management:** The security architecture also includes a guide detailing user account creation, what access to grant to the particular user, and what restrictions to impose. A security architecture must protect the whole IT infrastructure. As such, it should detail who can access sensitive data and who cannot. An accounting staff in charge of payroll processing, for example, should have access to employee timesheets and the payroll management software. Another accounting staff who handles the company's taxes don't necessarily need the same access. Limiting access to tools that contain sensitive data effectively reduces risks.

Security Auditing architecture

- **Security roles and their responsibilities:** Vital to any security architecture are the people who carry out every step within it. Who is responsible for the day-to-day operations of the security system? Who is in charge of maintaining specific applications and the whole network? Who are the end-users? Who will be the auditor of the overall security architecture? The answers to these questions should be part of the security architecture.
- **Auditing the security architecture:** The IT security landscape is continually changing, so there is a need to assess an organization's security architecture regularly. The auditors must make sure that the current architecture is still in line with the business goals and, at the same time, meets its needs. After the assessment, they should make the necessary adjustments to the security architecture.

Audit trail

An audit trail is **a series of records of computer events, about an operating system, an application, or user activities**. A computer system may have several audit trails, each devoted to a particular type of activity. Auditing is a review and analysis of management, operational, and technical controls.

- **Application-specific audit trail** – ideally, each application records business-relevant events. They may be logged in text files or in separate database tables. They allow reconstructing the history much better than the arbitrary noisy logging that is usually in place
- **Application logs** – this is a broader category as it includes logs that are not necessarily part of the audit trail (e.g. debug messages, exception stack traces). Nevertheless, they may be useful, especially in case there is no dedicated application-specific audit trail functionality
- **Database logs** – whether it is logged queries, change data capture or change tracking functionality, or some native audit trail functionality

Audit trail

- **Operating system logs** – for Linux that would include the /var/log/audit/audit.log (or similar files), /var/log/auth.log. For Windows, it would include the Windows Event logs for the Security and System groups.
- **Access logs** – access logs for web servers can be part of the audit trail especially for internal systems where a source IP address can more easily be mapped to particular users.
- **Network logs** – network equipment (routers, firewalls) generate a lot of data that may be seen as part of the audit trail (although it may be very noisy)

Audit Trail best practices

- Audit trails should be secured so they cannot be altered in any way.
- Limit viewing of audit trails to those with a job-related need.
- Protect audit trail files from unauthorized modifications.
- Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.
- Copy logs for wireless networks onto a log server on the internal LAN.
- Use file integrity monitoring/change detection software (such as Tripwire) on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

Pros and cons of audit trail

Pros

- Encourages user accountability and compliance
- Helps maintain a well-functioning economy
- Protects against fraud
- Improves security

Cons

- Costliness in terms of time and money
- Can slow business operations
- Requirements may be too rigid

Implementing Logging function

1. **Define your need to log and monitor:** Determining why the organization wants a logging solution will define what you need to log
    - Compliance requirement
    - Local laws and regulations
    - Incident response requirements
2. **State what needs to be logged and how it needs to be monitored:** Determines whats needs to be captured and what events to be logged
    - An actor(who : username, IP address)
    - An action(What : read/write on which resources)
    - A time(when : timestamp)
    - A location (Where : geolocation, browser,code scripts)

Implementing Logging function

3. Identify assets and events that need to be monitored:

- Needs to identify which systems/applications should be monitored and what level of monitoring is required.
- Classification of data and system according to organizations statutory,regulatory or contractual requirements
- Classifications may differ from your security system classifications or your business data classifications

4. Determine the right solution for logging and monitoring:

- Automate as much as possible of monitoring process
- Constantly tune your alerts and log sources as threats evolve
- Ensure that log and alerts are generated in standardized format

Implementing Logging function

5. Design logging and monitoring systems with security in mind:

- Anonymize sensitive information from event logs beforehand, to prevent sensitive information from being logged in plain text (e.g., PHI/PII information)
- Enforce role-based access controls
- Perform log integrity checks to ensure that logs are not tampered with
- Apply encryption at rest and transit
- Follow the principle of least privilege when configuring log sources
- Sanitize logs before storing and processing
- Include capabilities for high availability and redundancy

Implementing Logging function

6. Adopt organization wide logging and monitoring policies:

- This ensures consistency and that protocols and procedures are followed in logging
- Policies with a strong mandate and corporate backing ensures that logging and monitoring practices are followed

7. Establish active monitoring, alerting and incident response plan:

- Establish an incident response plan and rehearse at regular interval
- Trigger alerts in an adequate amount of time
- Take active automated action on the alerts

Audit Trail analysis

- **System-level audit trails:** If a system-level audit capability exists, the audit trail should capture, at a minimum, any attempt to log on (successful or unsuccessful), the log-on ID, the date and time of each log-on attempt, date and time of each log-off, the devices used, and the function(s) performed once logged on (e.g., the applications that the user tried, successfully or unsuccessfully, to invoke).
- **Application-level audit trails:** Application-level audit trails can capture information not tracked within system-level audit trails. In general, application-level audit trails monitor and log user activities, including data files opened and closed, specific actions, such as reading, editing, and deleting records or fields, and printing/downloading reporting.
- **User audit trails:** These can log things such as all commands directly initiated by the user, all identification and authentication attempts, and all files and resources accessed.

Audit trail benefits

- **Detect bad behavior such as misuse of systems and internal fraud:** When employees and contractors know that their activities are logged, it can detect people from misusing their privileged access to key systems containing sensitive information. Audit trails can also identify internal fraud by keeping track of different users and how they're interacting with a company's data.
- **Improve incident response:** Analysis of audit trails can help security teams reconstruct events after a problem has occurred, and learn from those events to improve their responses to future security incidents.
- **Intrusion detection:** Audit trails can help security staff identify moments when intruders are attempting to penetrate into systems and do harm.