UNIT-2

⇒ Hashing

⇒ Public key cryptosystems

⇒ Private Vs Public block chain and use cases.

⇒ Hash puzzles

⇒ Extensibility of Block chain concepts

⇒ Digital identity verification.

⇒ Block chain neutrality (నిష్పక్షపాతం)

⇒ Digital art

⇒ Block chain environment.

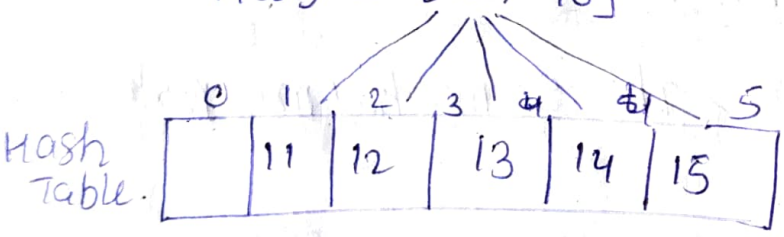
Hashing :-

⇒ Hashing refers to the process of generating a fixed-size output from an input of variable size using the mathematical formulas known as Hash function.

⇒ This technique determines an index of an item in a data structure.

List = [11, 12, 13, 14, 15]

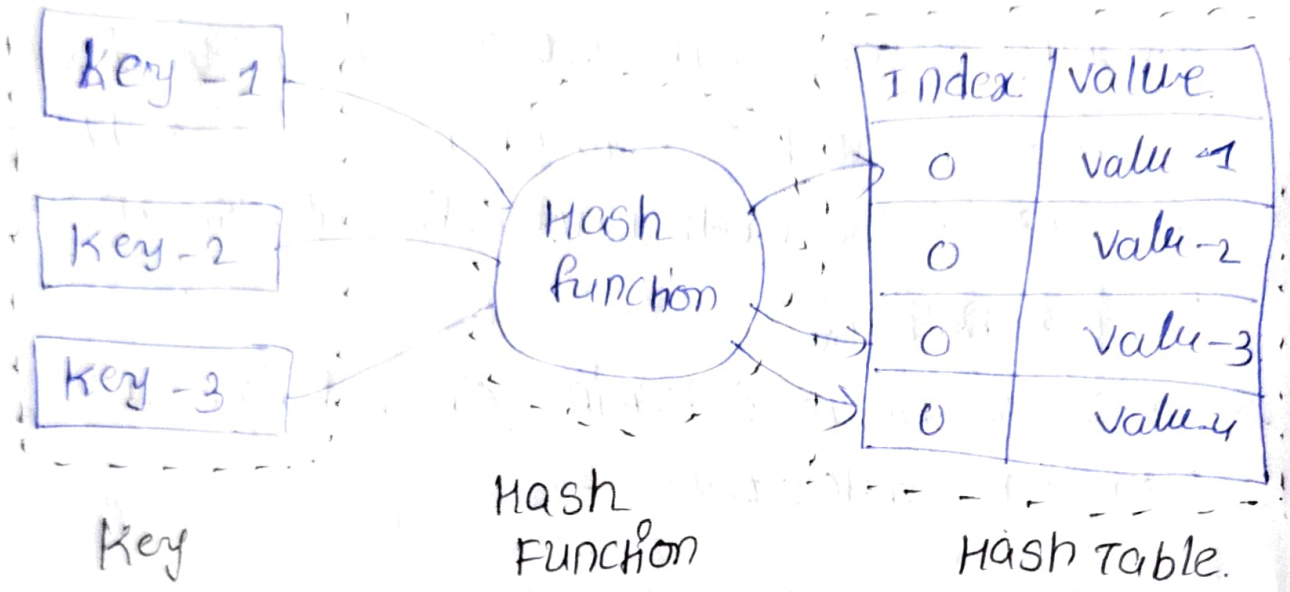
H(x) = [x % 10]



Components of Hashing:

There are majorly three components of hashing.

1. **Key:** A key can be anything string or integer which is fed as input in the hash function that determine location for storage of item.
2. **Hash Function:** The hash function receives the input key and returns the index of an element in an array called a hash table.
3. **Hash Table:** Hash Table is a data structure that maps keys to values using a special function called a hash function.



What is collision :-

⇒ In some cases the same key may produce same value.

⇒ this problem may be handled using some collision handling technology.

Advantages of Hasing:

* Key-value support:
  Hashing is ideal for implementing key-value.
* Fast Data retrievel:
  Hashing allows for quick access to element with constant time complexity.
* Efficiency:
  insertion, deletion and searching operations are highly efficient.

* memory usage reduction:

Hashing requires less memory as it allocates a fixed space for storing elements

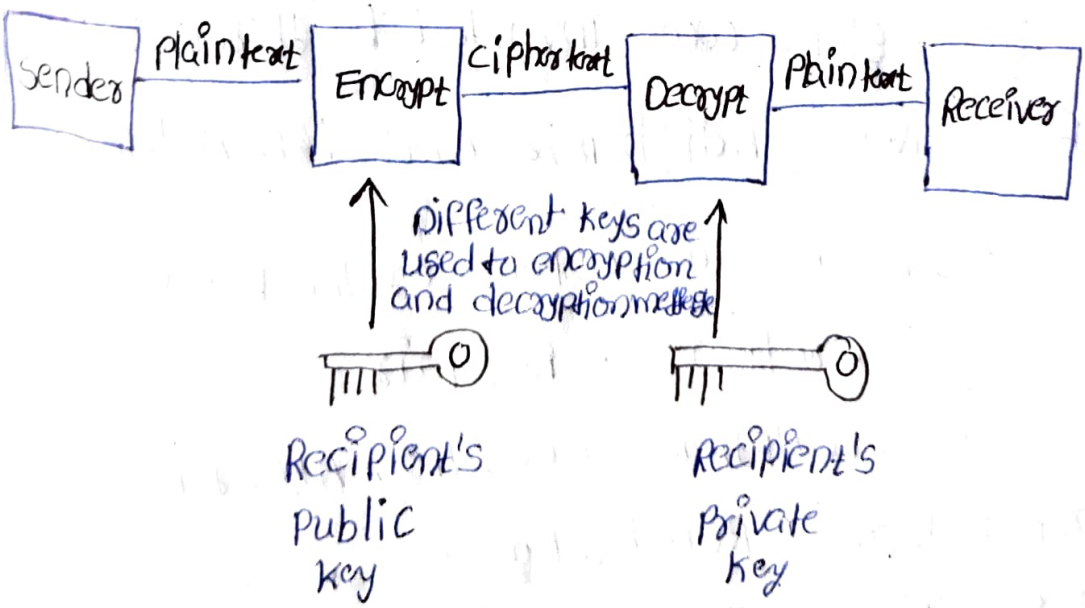
* scalability:

Hashing performs well with large datasets, maintaing constant Access Time.

* security and encryption:

Hashing is essential for secure data storage and integrity verification.

✓ Public key cryptosystems



⇒ The most important properties of public key encryption scheme are -

* Different keys are used for encryption and Decryption.

* Each Receiver Possess a unique decryption key. generally referred to as his Private key.

* The private and public keys are related mathematically it is not be feasible to calculate the private key from the Public key.

⇒ There are three types of Public key Encryption schemes.

1. RSA cryptosystem :-

⇒ this cryptosystem is one the initial system.

⇒ The system was invented by three scholars. Ron Rivest, Adishamir and Len Adleman.

⇒ we will see two aspects of the RSA cryptosystem
  * generation of key pair
  * Encryption - decryption Algorithms.

Generation of RSA key pair :-

1) select two prime numbers p & q.
2) calculate $n = pq$
3) calculate $\phi(n) = (p-1)(q-1)$
4) find integer e (Public key)
   $\gcd(\phi(n), e) = 1$ where $1 < e < \phi(n)$

5) Calculate 'd' (Private Key)

$$d < \phi(n).$$

$$ed = 1 \bmod \phi(n).$$

6) Perform Encryption by using.

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

7) Perform Decryption by using

$$M = c^d \bmod n.$$

ElGamal Cryptosystem :-

⇒ ElGamal cryptosystem, called Elliptic curve variant, is based on the Discrete Logarithm Problem.

⇒ ElGamal Algorithms are used for both Digital Signature as well as encryption.

ElGamal Algorithm :-

Global Public elements

q	prime number
α	$\alpha < q$ and α is primitive root of q.

Key Generation by Alice

Select Private X_A	$X_A < q-1$
calculate Y_A	$Y_A = \alpha^{X_A} \bmod q$
Public Key	$\{q, \alpha, Y_A\}$
Private key	X_A

Encryption by Bob with Alice's public key

Plain text	$M < q$
Select random integer k	$k < q$
Calculate K	$K = (Y_A)^k \bmod q$
Calculate C_1	$C_1 = \alpha^k \bmod q$
Calculate C_2	$C_2 = KM \bmod q$
Cipher text	(C_1, C_2)

Decryption by Alice with Alice's Private key

Cipher text	(C_1, C_2)
Calculate K	$K = (C_1)^{X_A} \bmod q$
plain text	$M = (C_2 K^{-1}) \bmod q$

3) Elliptic curve cryptography :-

⇒ Elliptic curve cryptography is based on sets of numbers that are associated with mathematical objects called elliptic curves.

⇒ there are rules for adding and computing multiples of these numbers.

Private Vs Public blockchain and use cases:-

Public Blockchain:-

⇒ Public blockchain are open networks that allow anyone to participate in the network.

⇒ In this type of blockchain anyone can join the network and read, write, or participate within the Blockchain.

⇒ The public blockchain is a decentralized

Private Blockchain:-

⇒ A Private Blockchain is managed by a network administrator and participants need consent to join the network.

⇒ In a Private Blockchain Transactions are private

Difference between Public and Private blockchain:

Basis of Comparison	Public Blockchain	Private Blockchain
Access	It is a Permissionless block chain.	It is a Permission block chain.
Network Actors	Don't Know each other	Know each other
Decentralized Vs Centralized.	Decentralized	centralized

order of magnitude	The order of magnitude of Public blockchain is lesser Then that private blockschain	The order of magnitude is more compared Public blockchain.
Security.	A Public network is more secure ducto decentralization and Active participation.	A private blockchain is more prone to hacks, risks
Energy consumption	A Public Blockchain consume more energy than a private block chain.	Private blockchains consume a lot less energy and power.
Attacks	In a public blockchain no one knows who each validater is and this increases The risk.	In a Private blockchain There is no chance of Attacks.
Examples	Bitcoin, Ethereum.	R_3 (Banks), EWF (Energy), corda.

, Hash Puzzles :-

⇒ Simply means that the hash puzzle is related to the world of cryptography, i.e. building unbreakable system.

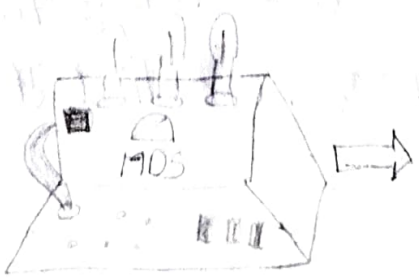
⇒ The best real world analogy to a hash puzzle is a fingerprint.

⇒ Imagine that you are given a fingerprint sample and you are asked to discover the height, weight and overall looks of the person to whom this fingerprint belongs.

⇒ To make it bit harder, Assume that there is no correlation blw fingerprints and other human features.

⇒ this process is hard to searching the fingerprints to others.

⇒ In a hash puzzle, the fingerprint that you are given is a list of characters like "dog" after which your task is to find the right person that produce the fingerprint.



⇒ when you have a machine that you put some digits in it, it produces an output of some other combination of digits

⇒ each time the machine checks ~~one~~ for one character to 16 different possible outputs.

Extensibility of Block chain concepts:-

⇒ Extensibility refers to the ability of a system to adapt (ಸಾಮರ್ಥ್ಯ) and evolve (ವಿಕಸನ) over time.

⇒ The Extensibility of blockchain technology allows for the development of new use cases beyond its original intent.

⇒ some of the challenges to be addressed are

1. Smart contracts:

⇒ Smart contracts are self-executing contracts with terms of the Agreement blw buyer and seller.

⇒ Smart contracts are a key innovation in Blockchain Technology, enabling the automation of complex Processes.

2. Scalability:

⇒ Scalability refers to the ability of a system to handle increasing amounts of work without impacting performance.

3. Interoperability:-

⇒ Interoperability refers to the ability of different blockchain networks to communicate and work together seamlessly.

4. privacy:-

⇒ privacy is a critical concern for many blockchain use cases, particularly those involving sensitive data.

5. Governance:

⇒ Governance refers to the system and processes in place to manage and regulate a blockchain network.

6. Sustainability:-

⇒ Sustainability refers to the ability of a blockchain network to operate over the long term.

⇒ Blockchain networks require significant computing power and energy consumption.

⇒ To improve sustainability

Some of the use cases are

1. Financial services:-

⇒ Blockchain technology has the potential to transform the financial services industry by enabling faster, more secure and more efficient transactions.

2. Supply chain management:-

⇒ Blockchain Technology can improve supply chain management by increasing transparency and Traceability, reducing fraud and counterfeiting and improving efficiency.

3. Health care:-

⇒ Blockchain Technology has the potential to Transform the healthcare industry by improving patient data management, reducing fraud, and increasing transparency.

4. Identity management:-

⇒ Blockchain Technology can improve identity management by reducing fraud, increasing security and improving privacy.

5. Voting System:-

⇒ Block chain Technology can improve voting system by increasing Transparency, reducing fraud and improving accuracy.

Digital Identity verification:

⇒ Identity verification is the concept of proving that an identity is a real one.

→ Identity verification is an important part of know your customer, customer due Diligence.

⇒ Identity verification is so important for preventing fraud and building Trust.

⇒ Digital identity verification focuses on collecting and verifying this personal information.

⇒ Typically At the point of on boading a new customer to business and matching it against trusted source and testing to ensure it is real, verifiable data or not.

⇒ identity verification must not interrupt or impede that customer.

⇒ The identity verification process is a important in a Data verification.

Data verification:-

⇒ Data-oriented Digital identity verification involves the matching of personal data-

⇒ The number of international identity data sources around the world can make this complex for any business trading

Document verification:-

⇒ Scanning and capturing information from a government issued identity document and verifying the document is an important document based approach.

⇒ These identity documents include passports, ID cards and driving licences.

What is identity Authentication;

⇒ The Identity Authentication referrs to the Authentication of Person.

⇒ mobile is another popular way to securely authenticate identity.

⇒ mobile number is a secure way of Authenticating a digital identity.

why is identity verification important:

⇒ Identity verification is the key to unlocking customer trust for successful companies.

⇒ To know your customer is a legal

realisement

Blockchain neutrality:-

⇒ Blockchain technology eliminates the need for trusted gatekeepers like banks to execute, verify and record Transactions.

⇒ neutrality principles, to ~~unto~~ unlock blockchain's competitive potential.

⇒ In the financial markets, their disruptive potential threatens both wall street banks and silicon valley venture capitalists.

Digital Art:-

⇒ Digital Art have been creating art digitally

⇒ The Thing that makes blockchain revolutionary for digital Art is the ability to prove Authenticity and Scarcity for digital Artworks.

⇒ Before blockchain, a digital artwork could be copied identically, making it difficult to build a market.

Authenticity:-

⇒ Blockchain ledger technology, which Acts as a Public record tracking system

⇒ The digital art prove Authencity of Artist.

Scarcity :-

⇒ through blockchain allow Authenticity of digital Art as well Bride Scarcity.

⇒ blockchain technology may create non-fungible token (NFT) for know the Scarcity.

⇒ this Tokens that represent a uniqure asset and therefore are not interchangeable.

what is NFT :-

⇒ NFT Stands for "Non-fungible Token"

⇒ Non-fungible means it's uniqure and can not be replaced with something else.

Example:

A bitcoin is fungible, trade one for another bitcoin.

⇒ At a very high level, most NFTs are part of the Ethereum blockchain.

Blockchain Environment:-

1. Supply chain management:

⇒ Blockchains can be used to track products from the manufacture to the shelf and help prevent waste, inefficiency, fraud.

⇒ they can also help consumers be better informed of how each product was made and shipped.

2. Recycling:

⇒ A Recycling program on the blockchain could encourage participation by giving a financial reward.

⇒ It would make it easy to transparently track data like volume, cost and profit and to evaluate the impact of each location,

3. Energy:-

⇒ Traditional Power grids are centralized, which can create inefficiencies in energy distribution.

⇒ A Peer to peer blockchain based energy system would reduce the need to transmit electricity over long distance.

4. Environmental Treaties:

⇒ Fraud and manipulation of data are also problems in this area.

⇒ Legal document storage on the blockchain could cutdown on fraud and manipulation.

5. Non-profits:

⇒ Blockchain enable funds to be Transferred without bank accounts.

⇒ It is possible to send money directly to the people.

6. Carbon Tax:

⇒ A blockchain-based reputation system could also give each company and product a score based.

1. changing incentives:

⇒ Blockchain technology can help both actions and incentives.

⇒ Incentives could completely change the drivers of our economy.