BT

▼ Unit I - Mathematical Foundation for Blockchain

Cryptography:
Cryptography is the practice of securing communication and data by converting it into a form that can only be read by someone who has the necessary key to decrypt it. It is divided into two main categories: Symmetric Key Cryptography and Asymmetric Key Cryptography.

Symmetric Key Cryptography:

- In symmetric key cryptography, the same key is used for both encryption and decryption.
- It's also known as secret-key or private-key cryptography.
- The key must be kept secret between the sender and receiver.
- Common symmetric algorithms include Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

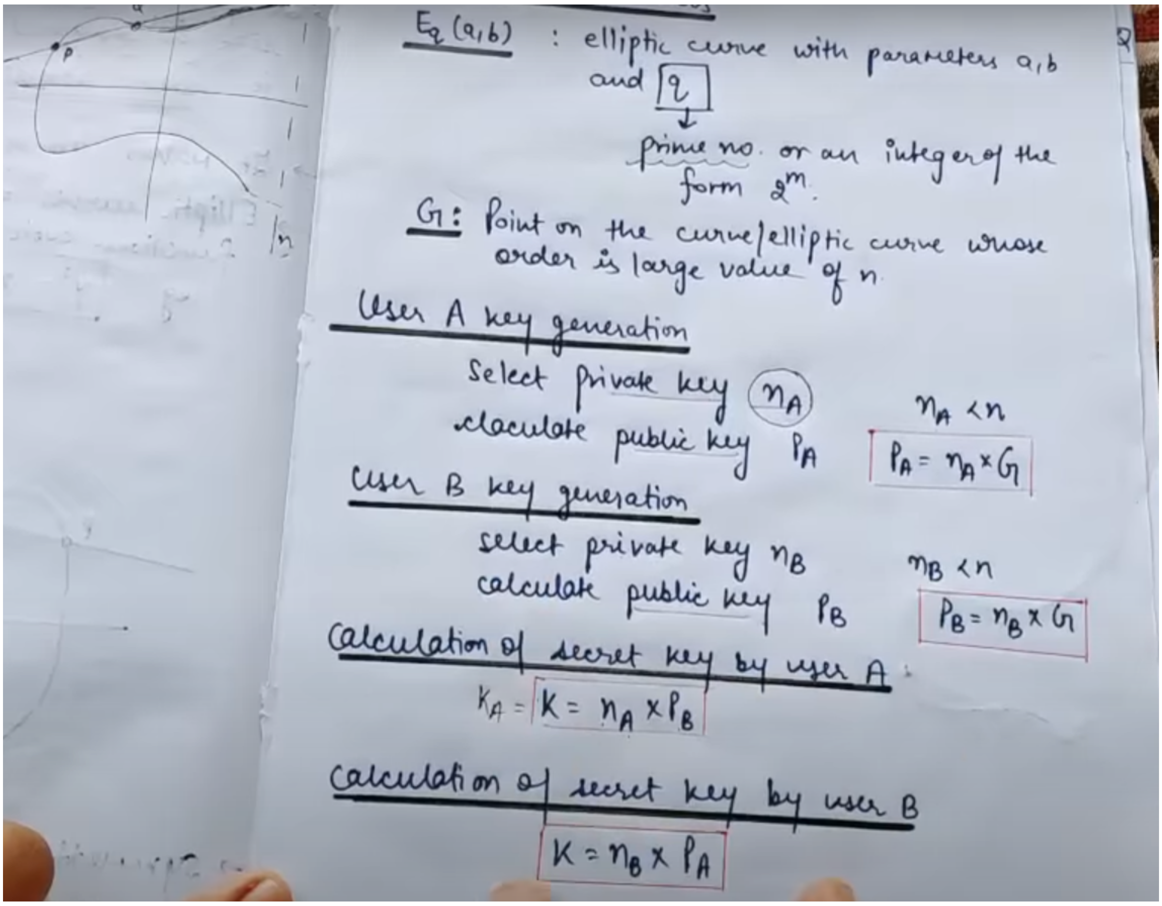
Asymmetric Key Cryptography:

- In asymmetric key cryptography, a pair of keys (public and private keys) is used for encryption and decryption.
- The public key is shared openly, while the private key is kept secret.
- Data encrypted with the public key can only be decrypted with the corresponding private key, and vice versa.
- Common asymmetric algorithms include RSA (Rivest-Shamir-Adleman) and Elliptic Curve Cryptography (ECC).

Elliptic Curve Cryptography (ECC):

- ECC is a type of asymmetric cryptography that uses the mathematics of elliptic curves for key exchange and encryption.
- It offers strong security with relatively small key sizes, making it efficient for resource-constrained devices like mobile phones.

- ECC is widely used in modern encryption protocols, including SSL/TLS for secure web communication.
- The curve is a mathematical curve defined by an equation in the form of `y^2 = x^3 + ax + b`. The curve is typically drawn as a set of points.



$E_q(a,b)$: elliptic curve with parameters a, b and $\boxed{q}$

↓

prime no. or an integer of the form 2^m.

G: Point on the curve/elliptic curve whose order is large value of n.

User A key generation

Select private key n_A $n_A < n$

claculate public key P_A $\boxed{P_A = n_A \times G}$

User B key generation

select private key n_B $n_B < n$

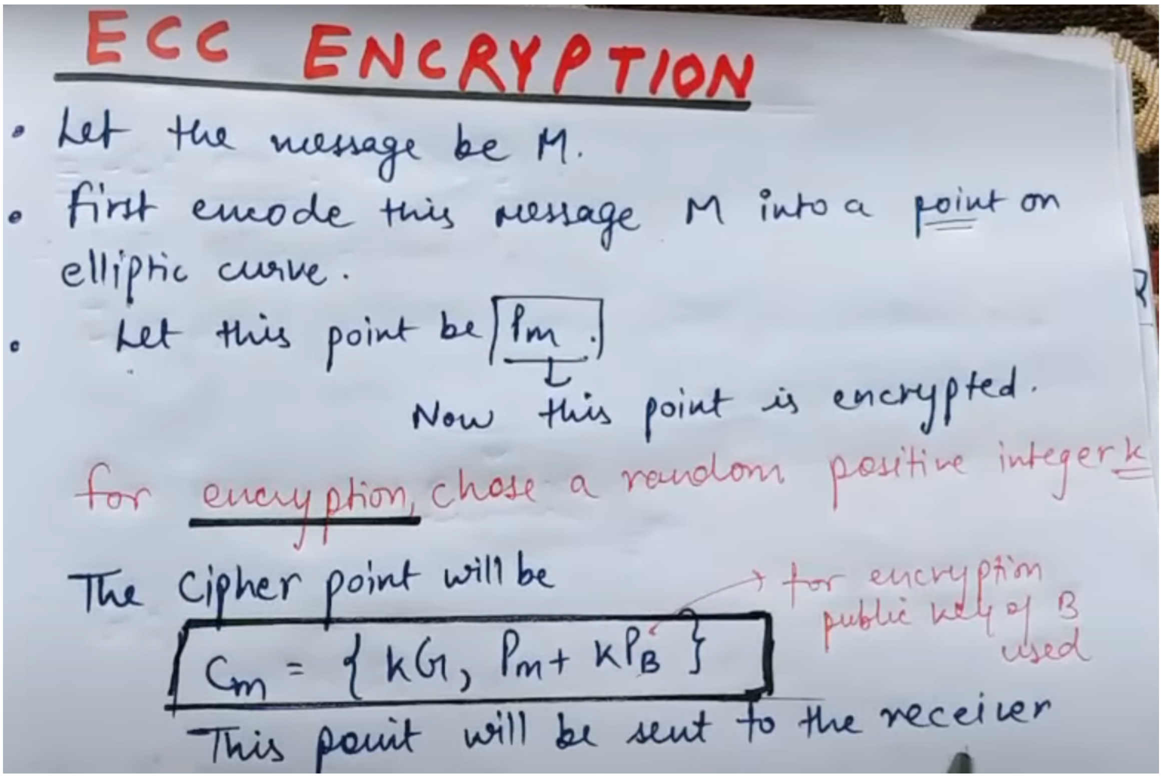
calculate public key P_B $\boxed{P_B = n_B \times G}$

Calculation of secret key by user A

$K_A = \boxed{K = n_A \times P_B}$

Calculation of secret key by user B

$\boxed{K = n_B \times P_A}$



ECC ENCRYPTION

- Let the message be M.
- First encode this message M into a point on elliptic curve.
- Let this point be P_m.

Now this point is encrypted.

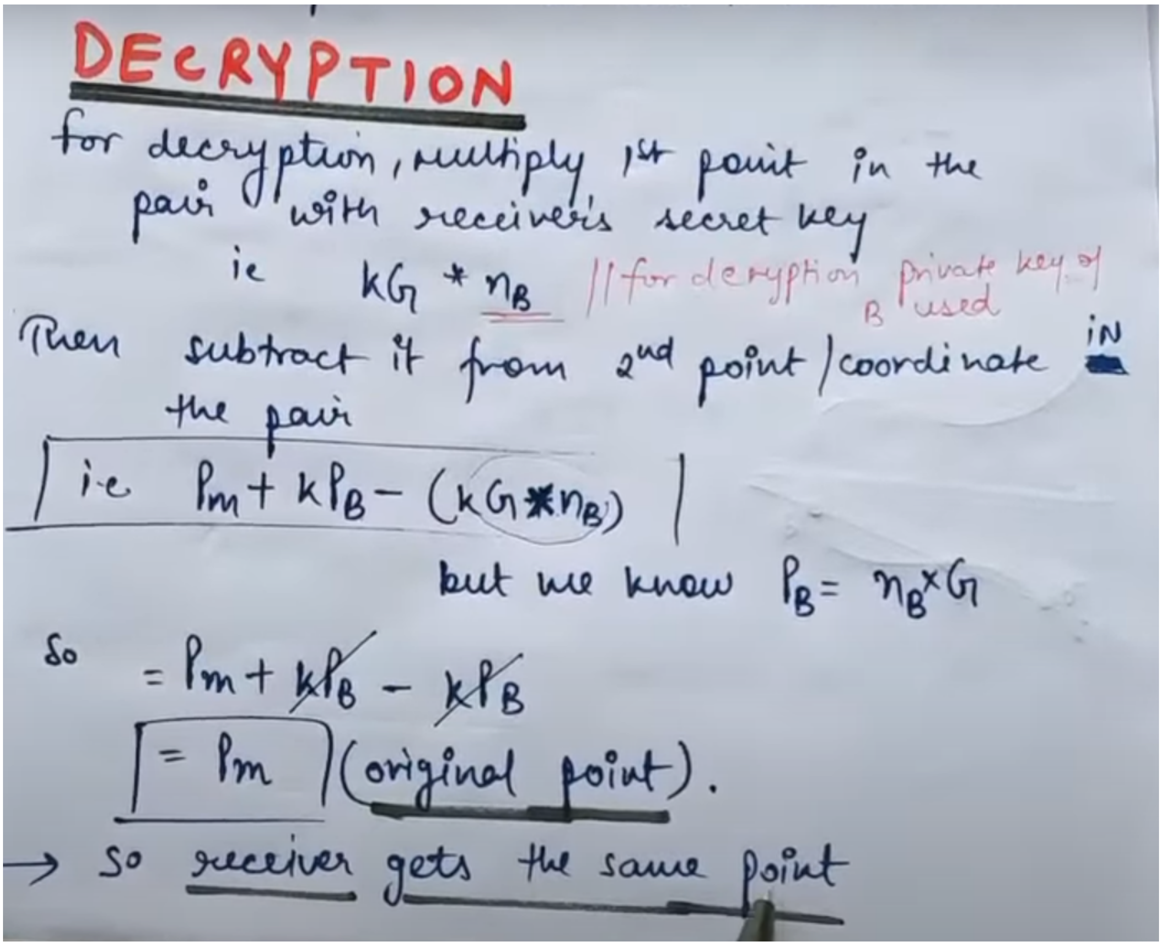
for encryption, chose a random positive integer k

The cipher point will be

$$\boxed{C_m = \{kG, P_m + kP_B\}}$$

for encryption public key of B used

This point will be sent to the receiver



DECRYPTION

for decryption, multiply 1st point in the pair with receiver's secret key

ie $kG * n_B$ //for decryption private key of B used

Then subtract it from 2nd point/coordinate in the pair

$$\boxed{\text{i.e } P_m + kP_B - (kG * n_B)}$$

but we know $P_B = n_B \times G$

So $= P_m + \cancel{kP_B} - \cancel{kP_B}$

$\boxed{= P_m}$ (original point).

→ So receiver gets the same point

Cryptographic Hash Functions (SHA256):

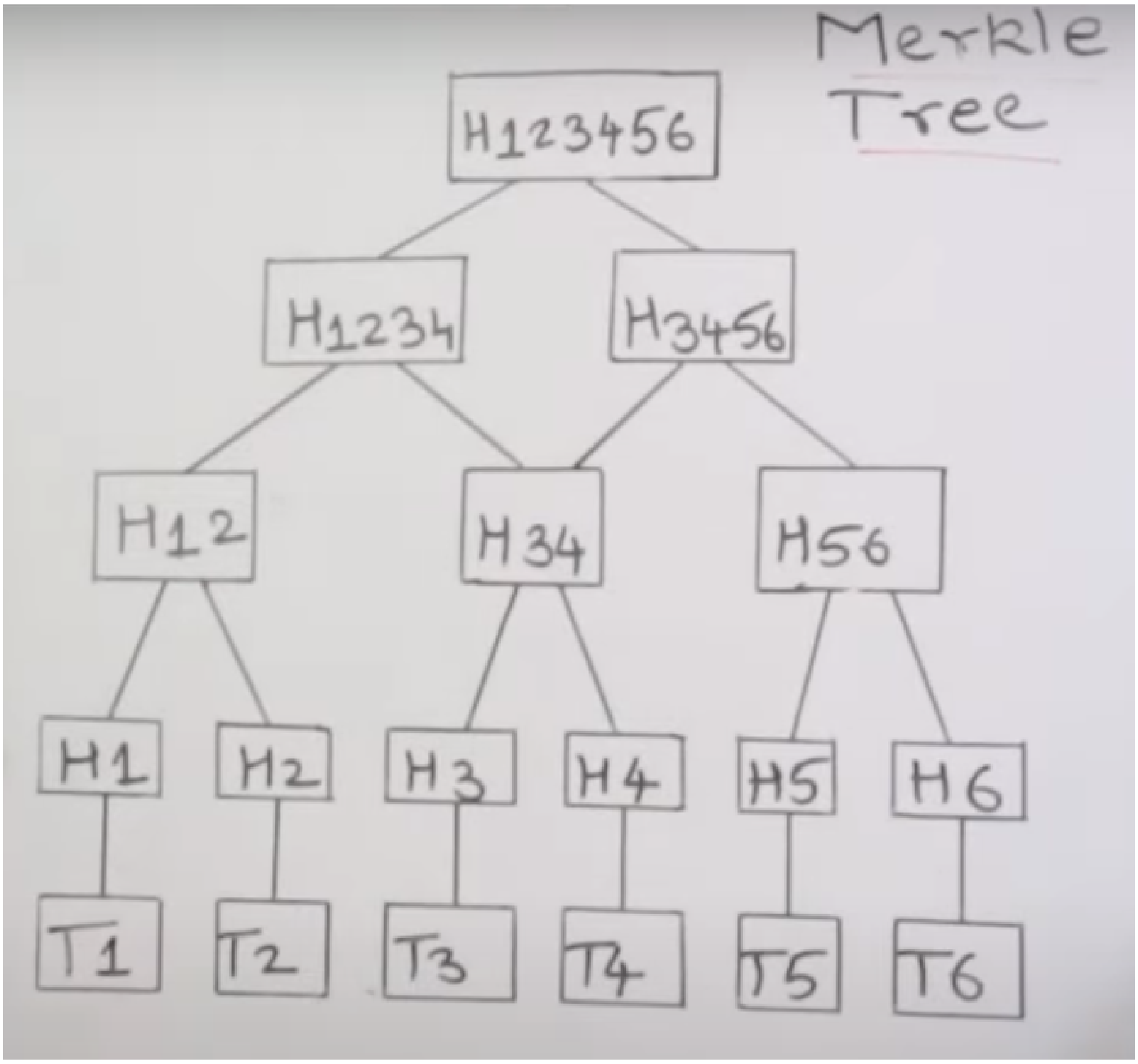
- Cryptographic hash functions are one-way mathematical functions that take an input (or "message") and produce a fixed-size string of characters, which is typically a hexadecimal number.
- The output, called a hash value or digest, is unique to each unique input.
- SHA-256 (Secure Hash Algorithm 256-bit) is a popular cryptographic hash function known for its collision resistance and security. It's used in blockchain technology, digital signatures, and data integrity verification.

Digital Signature Algorithm (DSA):

- DSA is a public-key cryptography algorithm used for digital signatures and authentication.
- It involves generating a pair of keys (public and private) and signing a document with the private key to prove its authenticity.
- The recipient can verify the signature using the sender's public key.
- DSA is widely used in secure communications and document verification.

Merkle Trees:

- A Merkle tree is a data structure used in cryptography and distributed systems to verify data integrity efficiently.
- It's built by recursively hashing pairs of data (usually chunks or blocks) until a single root hash is obtained.
- If any piece of data in the tree changes, it will result in a different root hash, allowing quick detection of tampering or corruption.
- Merkle trees are essential in blockchain technology, ensuring the integrity of the entire transaction history.



▼ Unit II - Feature Engineering

History of Blockchain:

- The concept of blockchain technology originated in 2008 when an individual or group using the pseudonym Satoshi Nakamoto introduced it in the Bitcoin whitepaper. Bitcoin's blockchain was the first practical implementation of blockchain technology.

Centralized vs. Decentralized Systems:

- **Centralized Systems:** In centralized systems, a single central authority or entity has control over the system, including data and decision-making. Examples include traditional banking systems and centralized databases.

- **Decentralized Systems:** In decentralized systems, control and data are distributed across a network of nodes. No single entity has complete control, making it more resistant to censorship and single points of failure. Blockchain is an example of a decentralized system.

Layers of Blockchain:

Blockchain Layer	Description	Key Functions	Examples
Application Layer	Top layer for user interaction and DApps	- Provides user interfaces - Executes smart contracts - Manages user wallets and identities	Ethereum DApps, Wallets, Blockchain Games
Execution Layer	Responsible for executing smart contracts and transactions	- Validates and executes smart contracts - Manages state transitions and ledger updates - Implements consensus mechanisms	Ethereum Virtual Machine (EVM)
Semantic Layer	Defines communication rules, data structure, and smart contract interaction	- Defines data format and structure - Enforces consensus rules and network protocols	Ethereum Solidity Programming Language
Propagation Layer	Manages the propagation and dissemination of transactions and blocks	- Relays transactions to network nodes - Ensures data synchronization	Data Propagation in Bitcoin, Ethereum Networks
Consensus Layer	Ensures agreement on transaction validity and block creation	- Implements consensus algorithms such as Proof of Work (PoW) or Proof of Stake (PoS)	Bitcoin PoW, Ethereum PoS

"Consensus Layer" is considered an integral part of the "Execution Layer." This is because the consensus mechanism, which is responsible for validating and confirming transactions and blocks on the blockchain, is closely tied to the execution of smart contracts and ledger updates.

Why is Blockchain Important?

- **Security:** Blockchain provides robust security through cryptography and decentralization, making it difficult for malicious actors to tamper with data.

- **Transparency:** Transactions on the blockchain are transparent and can be audited by anyone.
- **Trust:** It eliminates the need for intermediaries, fostering trust in peer-to-peer transactions.
- **Decentralization:** It reduces reliance on central authorities, promoting censorship resistance and resilience.
- **Efficiency:** Blockchain can streamline processes, reduce fraud, and increase efficiency in various industries.

Limitations of Centralized Systems:

- **Single Point of Failure:** Centralized systems have a single point of failure, making them vulnerable to outages or attacks.
- **Lack of Transparency:** Users often have limited visibility into how data is managed and transactions are processed.
- **Security Concerns:** Centralized systems can be targets for cyberattacks.
- **Trust Dependency:** Users must trust a central authority to manage and protect their data.

Blockchain Adoption So Far:

- Blockchain adoption has been significant in various sectors, including finance, supply chain, healthcare, and government.
- Cryptocurrencies like Bitcoin and Ethereum have driven blockchain awareness and adoption.
- Many organizations are exploring blockchain for its potential to improve transparency, traceability, and security.

Industry Sector	Blockchain Applications
Finance and Banking	- Cryptocurrencies for digital assets and investments
	- Cross-border payments and remittances
	- Smart contracts for automated financial agreements
Supply Chain and Logistics	- Provenance tracking for product traceability
	- Streamlined logistics, reduced paperwork

Healthcare	- Secure patient health records with data control
	- Drug traceability and authenticity verification
Government	- Enhanced election security with blockchain voting
	- Secure digital identities for citizens
Real Estate	- Property transfer and ownership records on blockchain
	- Tokenization of real estate for investment
Energy Sector	- Secure energy grid management
	- Tracking and trading carbon credits on blockchain
Education	- Credential verification for academic degrees
	- Secure and tamper-proof academic records
Entertainment and Intellectual Property	- Fair compensation for artists and creators
	- Content distribution and copyright protection
Agriculture	- Food safety through product origin tracking
	- Transparent agricultural supply chain
Emerging Use Cases	- Non-fungible tokens (NFTs), digital collectibles
	- Decentralized finance (DeFi) platforms
	- Decentralized autonomous organizations (DAOs)