1.

Q1> List and explain advantage of ECC ?

Ans: Elliptic Curve Cryptography (ECC) is a type of public-key cryptography based on the algebraic structure of elliptic curves over finite fields.

Here are some of its advantages:

1. ECC offers the same level of security as other public-key cryptography systems (like RSA) but with much smaller key sizes.
2. ECC requires less computational power, leading to faster encryption and decryption processes.
3. ECC uses smaller keys and shorter ciphertexts, which reduces the amount of data transmitted.
4. Devices using ECC consume less power due to the reduced computational complexity.
5. ECC is well-suited for systems requiring high scalability.
6. ECC can be used with various cryptographic protocols and standards.

Q2> Differentiate between asymmetric and symmetric key cryptography ?

Ans:

| **Feature** | **Symmetric Key Cryptography** | **Asymmetric Key Cryptography** |
| --- | --- | --- |
| **Key Type** | Single shared key | Public and private key pair |
| **Speed** | Faster | Slower |
| **Key Management** | Challenging | Simplified |
| **Security** | Dependent on key secrecy | Enhanced by key pair separation |
| **Use Cases** | Encrypting large data volumes | Secure key exchange, digital signatures |
| **Examples of Algorithms** | AES, DES, 3DES | RSA, ECC, DSA |

Q3> Discuss properties of hash functions ?

Ans: Hash functions are an essential component of cryptography and computer science. They transform input data of any size into a fixed-size string of characters, which typically appears as a sequence of numbers and letters. Here are the key properties of hash function

Properties of Hash Functions:

1. **Deterministic**: The same input will always produce the same output.
2. **Fixed Output Size**: Regardless of the size of the input, the output (hash value) is always of a fixed length.
3. **Fast Computation**: Hash functions should be capable of quickly generating the hash value from the input data.
4. Small Changes in Input Produce Large Changes in Output.
5. **Collision Resistance**: It should be computationally infeasible to find two different inputs x1x\_1x1​ and x2x\_2x2​ such that H(x1) = H(x2) H(x\_1) = H(x\_2) H(x1​) = H(x2​).

2.

Q1> Explain Prapogation layer in blockchain ?

Ans: The propagation layer in blockchain technology is responsible for disseminating information across the network. It ensures that all nodes in the blockchain network receive the necessary data to maintain a consistent and up-to-date ledger. Here are the key aspects of the propagation layer:

Key Aspects of the Propagation Layer :

1. **Broadcasting Transactions**: When a transaction is initiated, it must be broadcast to the entire network. The propagation layer handles this by sending the transaction to neighboring nodes, which in turn relay it to their neighbors, ensuring that the transaction reaches all nodes in the network.
2. **Block Propagation**: Once a miner successfully mines a block, it needs to be propagated to the entire network. The propagation layer ensures that the new block is quickly shared with all nodes to maintain a consistent blockchain.
3. **Gossip Protocol**: Many blockchain networks use a gossip protocol for propagation. In this protocol, nodes randomly select a few other nodes to share new information with, and these nodes do the same, creating a spreading effect similar to how rumors or gossip spread in social settings.
4. **Latency and Bandwidth**: The efficiency of the propagation layer affects the overall performance of the blockchain network. Lower latency and higher bandwidth can speed up the propagation process, leading to quicker transaction confirmations and block validations.

Q2> Discuss evolution of the Blockchain ?

Ans:

1. The evolution of blockchain technology began with foundational concepts in cryptography, such as Merkle trees and the Byzantine Generals Problem, which laid the groundwork for secure and distributed data structures.
2. This groundwork culminated in 2008 when Satoshi Nakamoto introduced Bitcoin, the first practical application of blockchain, in a whitepaper.
3. Bitcoin's success as a decentralized digital currency led to the development of Blockchain 1.0, primarily focused on cryptocurrencies. In 2015, Ethereum, proposed by Vitalik Buterin, marked the advent of Blockchain 2.0 by introducing smart contracts, which allowed for programmable and self-executing transactions, significantly broadening blockchain's potential applications.
4. This period saw rapid growth and the emergence of decentralized applications (dApps). More recently, Blockchain 3.0 has focused on improving scalability, interoperability, and sustainability, with innovations like proof-of-stake consensus mechanisms and advanced privacy features, driving adoption across diverse industries beyond finance, including supply chain, healthcare and governance.

Q3> Differentiate Centralized and Decentralized ?

Ans:

| **Feature** | **Centralized Systems** | **Decentralized Systems** |
| --- | --- | --- |

|  |  |  |
| --- | --- | --- |
| **Control** | Single central authority | Distributed among multiple nodes |

|  |  |  |
| --- | --- | --- |
| **Decision-Making** | Centralized at the top | Collective and consensus-based |

|  |  |  |
| --- | --- | --- |
| **Data Storage** | Centralized servers | Distributed across multiple nodes |

|  |  |  |
| --- | --- | --- |
| **Efficiency** | High efficiency, quick decisions | Lower efficiency, requires consensus |

|  |  |  |
| --- | --- | --- |
| **Security and Risk** | Single points of failure, higher risk | More resilient, lower risk |

|  |  |  |
| --- | --- | --- |
| **Scalability** | Potential scalability issues | Scalability challenges due to consensus |