UNIT-1
Mathematical foundation for Blockchain.

Q1) Define cryptography & its types.

→ a) Cryptography

- Cryptography is defined as storing or transferring encrypted data between senders & recievers on public or private networks such that only intended recipients can read it on recieving it.
- It is the study of using mathematics to encrypt & decrypt information or data to be stored or transmitted on insecure networks.
- It helps you store or transmit vital infoemation across public or private networks so that it can be percieved by the intended recipient exclusively.

* Following are the types of cryptography

1) Symmetrical Cryptography
2) Asymmetrical cryptography
3) Hash Functions.

Q2. Compare symmetric & asymmetric cryptography.

	Symmetric	Asymmetric
1)	It uses single key	It uses public & private key
2)	Key exchange takesplace.	No need to exchange keys.
3)	Key must not be known to anyone else bat the sender & recievers.	Reciever's public key is known to everyone but private key is known to the reciever only.

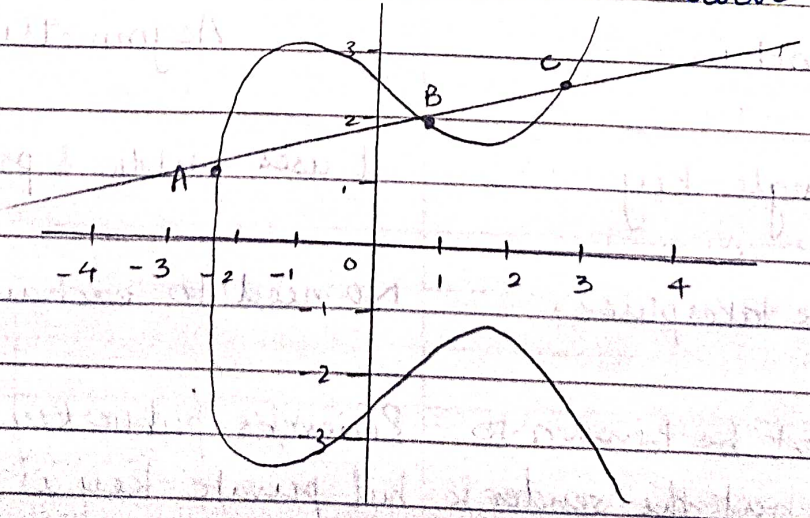
	Symmetric	Asymmetric
4)	Most commonly used algorithms are AES & DES.	Most commonly used algorithms are RSA & Diffie Hellmann Key Exc
5)	It takes less time to encrypt & decrypt the message.	It is slower than symmetric key cryptography.
6)	The no. of keys reqd is high	No. of keys reqd. is low

Q3. Write in brief about ECC, equation of ECC, why ECC is preferred over RSA.

→
- ECC stands for Elliptic Curve Cryptography.
- It is based on discrete logarithms problem founded upon elliptic curves over finite fields.
- An elliptic curve is a set of points that satisfy a specific mathematical equation.
- Elliptic curve equation is:

$$y^2 = x^2 + ax + b$$

- Any non-vertical line will intersect the curve in three places.



- ECC is frequently used for key exchanges & digital signatures

- ECC uses integer private keys that fall inside the field size range of the curve, which is generally 256 bits.
- The public keys in ECC are ECC points which are pairs of x, y co-ordinates.
- EC points may be reduced to only one co-ordinate plus 1 bit because of their unique characteristic.
- ∴ Compressed public key is 257 bit integer.
- The length of ECC keys is closely related to the underlying curve.
- The default key length for the ECC private keys is 256 bits however, many alternatives such as 233 bit & 192-bit are feasible.
- ECC has the advantage of requiring a smaller key size while yet offering the same level of security as RSA.

* Pros.

i) Shorter key length
Same level of security achieved at much shorter key length.

ii) Better security.

iii) Higher performance.

* Cons.

i) As it is relatively new field, all aspects are not explored yet

ii) Attacks still exist which can solve ECC, therefore not perfect.

Q4. What is symmetric key cryptography?

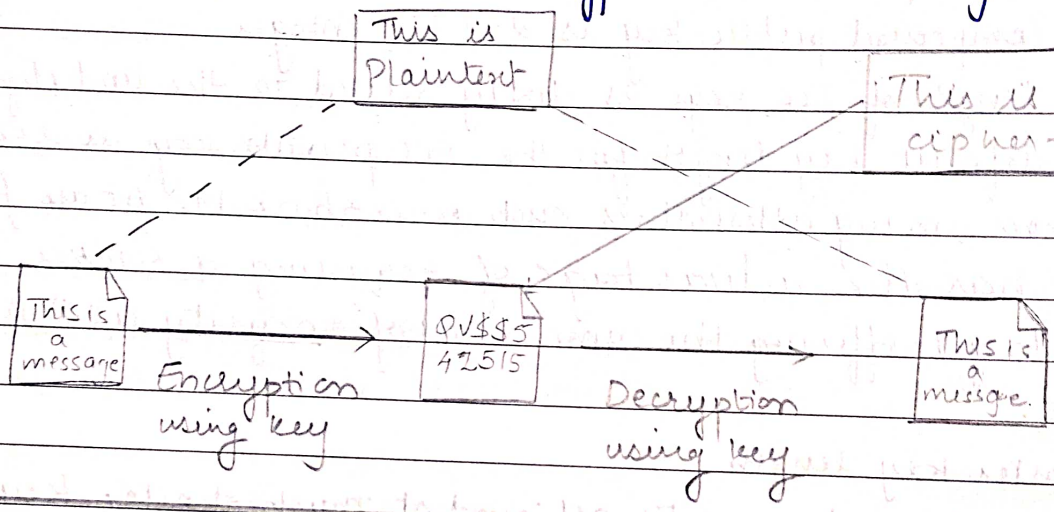
→ - Symmetric key cryptography is a type of cryptography in which sender & reciever share the single key to encrypt & decrypt the message.
- Here the sender & reciever know the secret key.
- Steps:

1) Sender & reciever share the secret key through some external means.

2) Sender encrypts the message (plaintext) using his copy of the

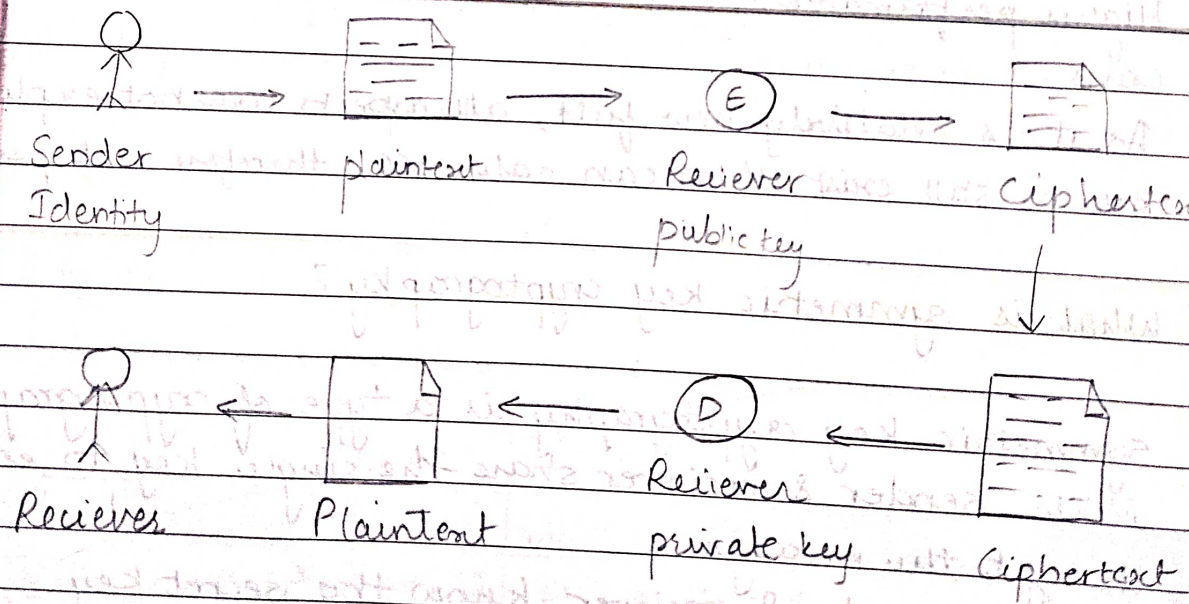
key at the sender's end. Here plaintext is ~~converted~~ encrypted to generate cipher text.

3) The ciphes text is then sent to the reciever over communication channel.
4) The recipient decrypts the ciphertext using his copy of the key.
5) Then the cipher text is decrypted back into original plain text



Q5. What is asymmetric key cryptography?

→



- Asymmetric key is also known as public key cryptography.
- It encrypts & decrypts data using both public & private keys.
- Steps:

1) Sender encrypts plaintext using recipient's public key

& encryption key function E to create ciphertext which is sent to the recipient.

2) The reciever uses public key of the reciever is publicly available & known to everyone.

3) Encryption mechanism converts the plaintext to cipher text.

4) This cipher text can be decrypted using reciever's private key.

5) The cipher text is sent to the reciever.

At reciever's end :

1) Reciever decrypts the cipher text using his private key.

2) The private key of reciever is known only to reciever.

3) Using the public key, it is not possible for anyone to determine the reciever's private key.

4) After decryption, cipher text converts back into readable plain text format--

Q6. Describe the steps to generate public & private keys in RSA.

→ i) Modulus generation

- Select p & q which are very large prime numbers.
- Calculate the value of n, $n = p \cdot q$.

ii) Generate co-prime

- Assume a number called e.
- e should satisfy certain condition that it should be greater than 1 & less than $(p-1)(q-1)$

iii) Generate the public key

- The modulus n & e are the pair of public key.
- The public key can be shared but p & q need to be secret.

iv) Generate private key

- Calculate private key 'd' by

$$ed = 1 \bmod (p-1)(q-1)$$

Q7 Explain general cryptography model with suitable digram.

→ A generic cryptographic model has the following terms:

1) Entity.
Either a person or system that sends, recieves or performs operations on data.

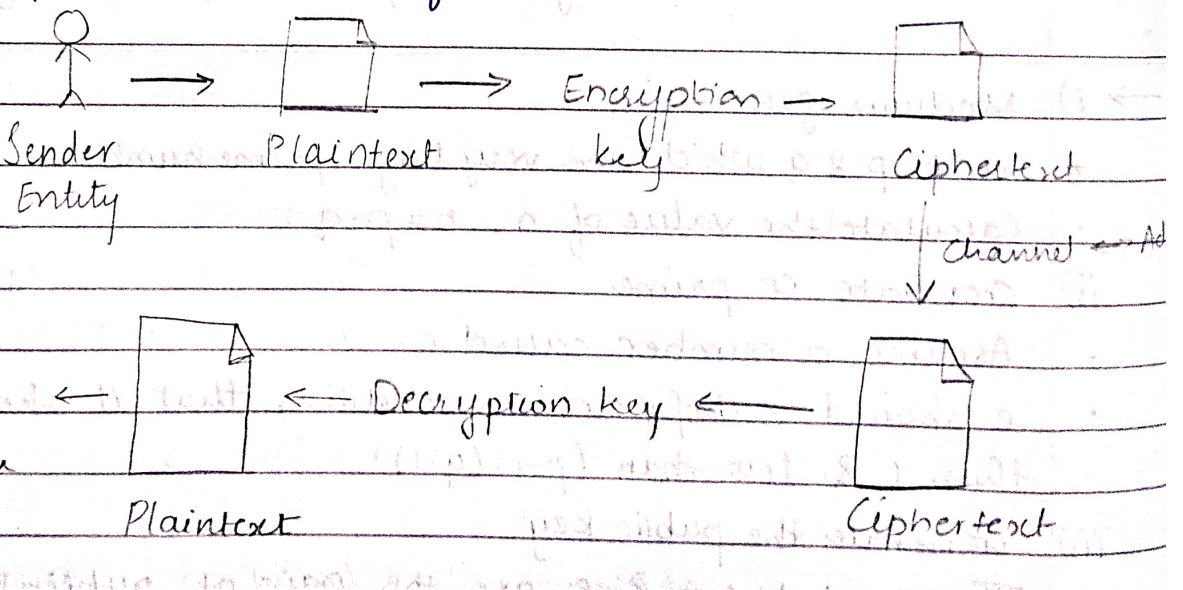
2) Sender.
An entity which transmits data.

3) Reciever
This is an entity which takes delivery of data.

4) Adversary
This is an entity which tries to circumvent the security service

5) Key
A key is data that is used to encrypt or decrypt other data

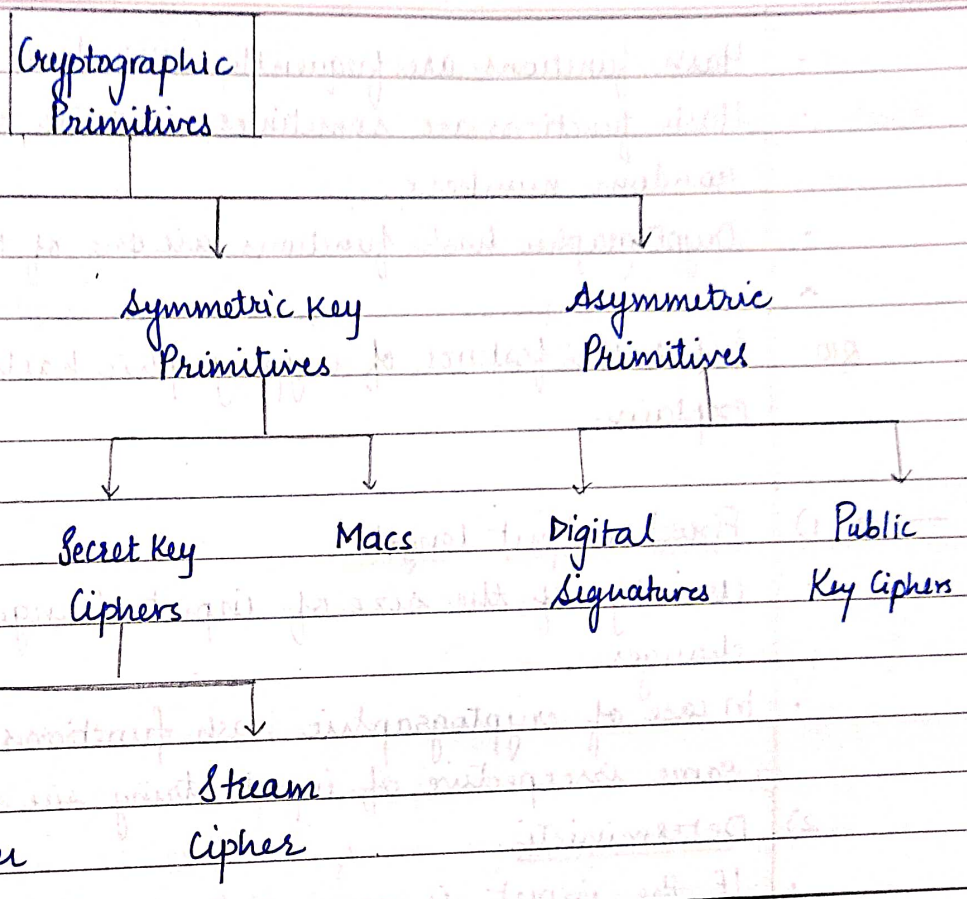
6) Channel
Channel provides a medium of communication between entities.



Q8. Draw & explain the taxonomy of cryptographic primitives

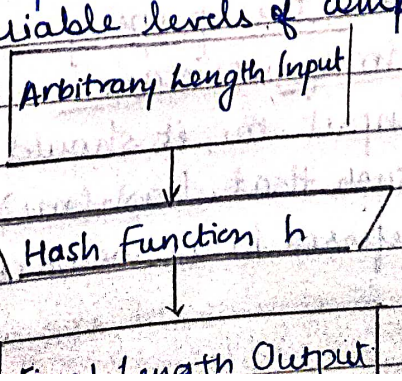
→ Cryptographic primitives are the basic building blocks of a security protocol or system.

~~A security primitive~~



Q9. State & explain Hash functions.

→ • Hash functions are used to convert infinitely lengthy ~~output~~ input texts into digests of fixed length.
• Hash functions offer the data integrity service & are keyless.
• It is a mathematical hash function used in cryptography.
• It transforms or "maps" a given set of data into a bit string of fixed size which is known as 'hash value'.
• A hash function combines message-passing capabilities of hash function with security properties.
• Hash functions have variable levels of complexity & difficulty.



- Hash functions are frequently utilised to offer data integrity services.
- Hash functions are sometimes used in applications to create pseudo-random numbers.
- Cryptographic hash functions are one of the key components of blockchain.

Q10. Enlist the features of cryptographic hash functions? State and explain.

→ 1) Fixed output length.
- Usually, if the size of input changes then size of output changes.
- In case of cryptographic hash functions, output string size remains same irrespective of input string size.

2) Deterministic
- If the input is same, output will also be the same.
- If the ~~fun~~ function is applied on the same input any number of times, the resultant answer will always be the same.

3) Easy computation.
- Hash functions are easy, efficient & fast one-way functions.
- It is required that hash functions be very quick to compute regardless of message size
- Efficiency may decrease if the message length is too long.

4) Pre-image resistance.
- Given a hash value h, it should be difficult to get any message m such that h = hash(m).
- Functions that lack this property are vulnerable to preimage attacks.

5) Second Pre-image resistance
- Given an input m_1, it should be difficult to find different input m_2 such that $hash(m_1) = hash(m_2)$
- It is also referred to as weak collision resistance

6) Collision resistance.
It should be difficult to find two messages m_1 & m_2 such that hash(m_1) = hash(m_2)
Such pair is called cryptographic hash function collision.

7) Avalanche effect:
A small change in input causes large change in output.

Q11. Explain SHA 256.

→ • SHA 256 stands for Secure Hash Algorithm 256.
• It is a cryptographic hash algorithm used for ~~convert~~ message, file & data integrity verification.
• It is a part of SHA-2 family of hash functions.
• It uses a 256 bit key to take a piece of data & convert it into a new, unrecognizable data string of fixed length.
• This string of random values & numbers is called hash value which is 256 bits in size.
• Block-size is 512 bits & has a word size of 32-bits.
• Output is a 256 bit digest.
• Algorithm works in 8 steps:

a) Pre-processing
1) If a block's size/length is less than 512 bits, padding of message is used to increase it to 512 bits.
2) Parsing the message into 512 bits which separates message & padding into ~~different blocks~~. equal blocks.
3) Creating the intial hash value, which is made up of the first 32 bits of the fractional portions of the square roots of the first 8 prime integers.
The first hash value is composed of eight 32-bit words.

b) Hash computation
1) Following that, each message block is analysed one at a time

- It takes 64 rounds to compute the whole hash result.
- To ensure that no two rounds are the same, each round uses slightly different constants.

2) The message schedule has been set.
3) Eight operational variables are initialised
4) A calculation is made for intermediate value.
5) After the message has been processed, output hash is produced.

Q12. How the digital signature & verification is carried out? ~~(with RSA digital signature algorithm)~~

→ • DSA stands for Digital Signature Algorithm.
- It is used for digital & signature & its verification.
- It is based on mathematical concept of modular exponentiation & discrete logarithm.
- It has four operations

1) Key generation
2) Key distribution
3) Signing
4) Signature verification

- Steps at signer's end

a) Message / ~~hash~~ data is hashed using hashing function to create a digest.
b) Sender uses his private key to sign the generated digest using the signature algorithm.

- Steps at reciever's end.

a) Recipient on recieving data & signature runs a verifier algo & used sender's public key.
b) If the generated hash value ~~for~~ matches with the hash value generated from earlier hashing, then recipient is satisfied with recieved data & signature

If matching fails, the signature of sender is not valid.

* Digital signature process is divided into two parts:

1) Signature Generation
a) Generating a pair of public keys & providing a key by sender of the message.
b) Generating message digest from message using a hash function.
c) Generating digital signature from message digest with private key.
d) Sending the message, the digital signature & public key to the reciever.

2) Signature Verification
a) Generating the message digest from message using same hash function.
b) Verifying digital signature with message digest using public key.
c) RSA & DSA are the algos used to generate & verify digital signature using public keys.

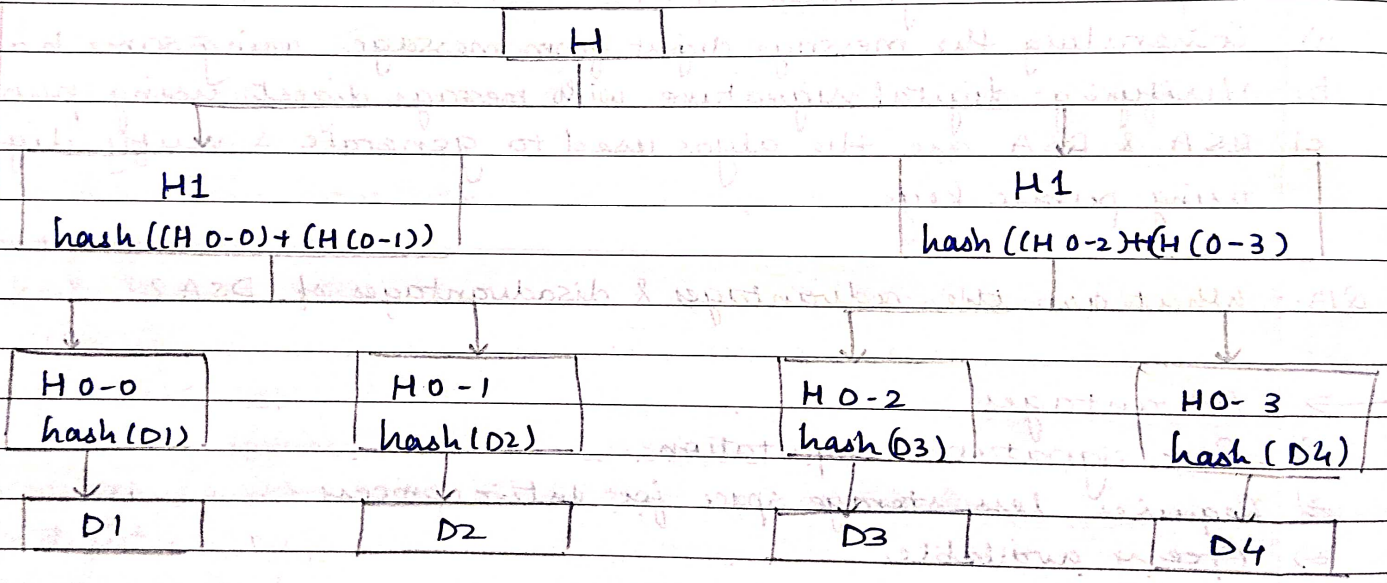
Q13. What are the advantages & disadvantages of DSA?

→ Advantages
1) Fast signature computation.
2) Requires less storage space for entire process
3) Freely available
4) Small signature length
5) Observation in real time
6) Non-invasive
7) Accepted globally for legal compliance.
8) Time-efficient

• Disadvantages
1) Process does not include key exchange capabilities
2) Underlying cryptography must be new to ensure its strength.

Q14. What are Merkle Trees? Explain the structure of a Merkle tree

→ • A Merkle tree is a binary tree containing hash pointers.
• The Merkle tree is also known as Hash tree
• It is a kind of data structure used for data synchronisation & verification.
• Each non-leaf node of the tree data structure is a hash of the nodes it contains/has as children.
• The leaf nodes are all equally deep & as far to the left as they can be.
• It employs hash functions to preserve integrity of data.



• An input of data broken up into blocks labelled D1 to D4.
• Each blocks ~~are~~ is hashed using some hash function.
• Then each pair of nodes are recursively hashed until the we reach the root node, which is a hash of all nodes below it
• The hash value at root node is called Merkleroot.