1. Before we have discussed about Encryption Algorithms (DES, DES3, AES, RSA) and Symmetric Key Encryption (DES, DES3, AES).
2. Encryption is usually used for making data unreadable for 3rd party.  
   The encrypted data when wired over network may be easily changed or compromised.   
   In that case, the receiver will not be reading the original data or reading it with an error.

A diagram of a blockchain

Description automatically generated

1. **That is where Hash comes in**.
   1. Hash is fixed length String.
   2. Its length can be 128, 160-bit etc. based on the algorithm used to create it.
2. **How do Hash Algo works**?
   1. It takes input data of any length.
   2. When the hash function is applied, it produces fixed length hash.
   3. This hash is irreversible because from this hash we can not go back to the input data.
   4. Why?
   5. Because same hash may be created for unlimited for different inputs.  
      That is why Hash Function is One-Way.
3. **Characteristics of Hash**?
   1. We cannot go back to the input.
   2. A slight change (a single character) in the input, the output hash will also change.
   3. The hash function does not require any key. Only Hash Function and Input enough.
      1. Still there are some hash functions which require keys.
4. **Why do we need Hash and Hash Functions?**
   1. Hash is used to check the integrity of the data transferred to the receiver by the receiver side.
   2. After encryption of data, the data as input is given to hash function and a hash is generated.
   3. That generated hash plus the encrypted data are sent to the receiver.
   4. The receiver will again use the same hash function to re-generate the hash and will compare it with the received one.   
      If both are same it means during the transmission over network, it was not mutated by someone, and the data received as released by the sender.
   5. Hash functions like MD5 and SHA1 do not use a key to generate hash function.
   6. **That is purpose of the key in hashing**?
   7. 
   8. See, encrypted data + Hash Key together given as input to hash function to generate hash.   
      The same hash key must be in the receiver side.   
      If receiver also generates same hash with the hash key, it means the data is coming from the authenticated sender.