1. **Answer to the questions are below**

i) Data communications is the process of using computing and communication technologies to transfer data from one place to another, or between participating parties.
Data security ensures that our data is only accessible by the intended receiver and prevents any modification or alteration of data.It is the process of protecting digital data and preventing data loss through unauthorized access.

ii) A transposition cipher is a method of encryption which scrambles the positions of characters without changing the characters themselves.
Transposition ciphers reorder units of plaintext (typically characters or groups of characters) according to a regular system to produce a ciphertext which is a permutation of the plaintex.
The Caesar cipher is based on transposition and involves shifting each letter of the plaintext message by a certain number of letters

iii) Hash works by mapping an arbitrarily-sized input for a fixed-size output in a process called compression. It is a mapping that is non-invertible. A hash function must align with two properties in order to be useful:
• One-way.
• Collision resistant.

iv) A stream cipher is an encryption technique that works byte by byte to transform plain text into code that's unreadable to anyone without the proper key.

A block cipher is a method of encrypting data in blocks to produce ciphertext using a cryptographic key and algorithm.

A block cipher breaks down plaintext messages into fixed-size blocks before converting them into ciphertext using a key. Encrypting information bit-by-bit. A stream cipher, on the other hand, breaks a plaintext message down into single bits, which then are converted individually into ciphertext using key bits.

v) When a person sends data through a document, it becomes important to identify his/her authenticity for security and safety reasons. Digital signatures are used for this identification. Authentication of the documents means to be aware of who created them and that they did not interfere during their transmission. These signatures are created using certain algorithms.
The Digital Signature Algorithm (DSA) is one of these. DSA is a type of public-key encryption algorithm, and it is used to generate an electronic signature. In DSA you use the public key for encryption and the private key for decryption.

vi) The requirements for digital signatures are:
• Each user should have the ability to generate their own signature on any selected document they chose.
• Each user should have the ability to efficiently verify whether or not a given string is the signature of another particular user.
• No one should have the ability to generate signatures on documents that the original owner did not sign