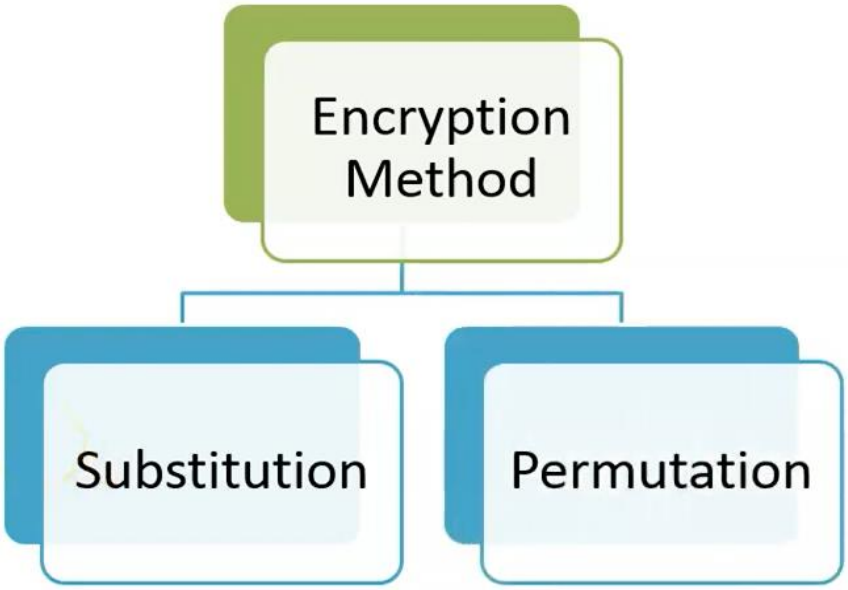
Encryption Methods

- There are two basic methods of encryption:



Confusion and Diffusion

- **Claude Shannon** introduced this two terms:

- **Confusion**
  - It is a technique of ensuring that a cipher text gives no clue about plain text.
  - It is used in block and stream cipher method.
  - Achieved by Substitution technique.
  - Ex: ABC → XYZ

- **Diffusion**
  - Increases the redundancy of the plain text by spreading it across rows and columns.
  - It is used in block cipher method.
  - Achieved by permutation known as Transposition technique.
  - Ex: ABC → CAB

No	Confusion	Diffusion
1	Cipher text cannot give the clue about plain text.	Increase the redundancy of plain text and generate cipher text.
2	Confusion technique is used in both block and stream cipher.	Diffusion technique is only used in block cipher.
3	Confusion hides the relation between the ciphertext and key.	Diffusion hides the relation between the ciphertext and the plaintext.
4	This technique is possible through substitution algorithm.	While it is possible through transportation algorithm.
5	If a single bit in the key is changed, all the bits in the ciphertext will also have to be changed.	In case a symbol in the plaintext is changed, several or all symbols in the cipher text will also have to be changed.