Feistel Cipher model is a structure or a design used to develop many block ciphers such as DES. Feistel cipher may have invertible, non-invertible and self invertible components in its design. Same encryption as well as decryption algorithm is used. A separate key is used for each round. However same round keys are used for encryption as well as decryption. 

## Feistel cipher algorithm

* Create a list of all the Plain Text characters.
* Convert the Plain Text to Ascii and then 8-bit binary format.
* Divide the binary Plain Text string into two halves: left half (L1)and right half (R1)
* Generate a random binary keys (K1 and K2) of length equal to the half the length of the Plain Text for the two rounds.

First Round of Encryption

* **a.**Generate function f1 using R1 and K1 as follows:

f1= xor(R1, K1)

* **b.**Now the new left half(L2) and right half(R2) after round 1 are as follows:

R2= xor(f1, L1)

L2=R1

Second Round of Encryption

* **a.**Generate function f2 using R2 and K2 as follows:

f2= xor(R2, K2)

* **b.**Now the new left half(L3) and right half(R3) after round 2 are as follows:

R3= xor(f2, L2)

L3=R2

* Concatenation of R3 to L3 is the Cipher Text
* Same algorithm is used for decryption to retrieve the Plain Text from the Cipher Text.