# Crypto FPGA

## EndGame - Version 1.0

Q1) An integral part of DES is Fiestel Structure. A Feistel Structure represents a non linear transformation that is invertible. DES contains a Feistel Structure in every round. Identify the corresponding Feistel Structure in DES and implement it for the first 4 bits of the plain-text (starting from the leftmost bit) in Verilog.

**Need for Feistel Structure** : Since all encrypting algorithms require decryption to recover the original information, it is essential to apply transformations which are invertible in order to get pre image of encrypted data. All linear transformations are invertible (for example x = Ay, where A represents an invertible matrix) Note that y may be recovered simply through $y = A^{-1}x$. However such linear transformations are vulnerable to chosen plain text attacks(GOOGLE!).
Therefore there is a need to get an invertible function which is non-linear. This is given by a Feistel Function.

---

To Be Continued...

ALL THE BEST!! - *V-M-S*