DES – Data Encryption standard

Block cipher – combine confusion and diffusion many times to build a strong block cipher. Confusion (look-up table), diffusion (permutation)

Feistel structure – Many of today’s ciphers are Feistel Ciphers

1st step: L0, R0 (64 bits -> 32 bits, 32 bits)

Round 1:

A picture containing text, blackboard, sign, green

Description automatically generated

(only) L0 is getting encrypted using an XOR operation

A picture containing text, blackboard

Description automatically generated

F Function

A picture containing text, blackboard, green

Description automatically generated