Cryptography - project proposal

Team Members:

- Nirbhay sharma (B19CSE114)
- Mayank Raj (B19CSE053)

Project Topic:

- paper: Linear Cryptanalysis of FF3-1 and FEA

Aim to study

The aim is to analyze and study the linear cryptanalysis of format preserving encryptions (FF3-1, FEA-1, and FEA-2), the format preserving encryption (FPE's) are methods to encrypt plain text in such a way that output is of same format as input, format preserving encryption finds applications in areas like credit card encryption etc. so in case of credit cards we want to encrypt a 16-digit credit card number to another 16-digit number, or encrypting a english word to some other english word etc. in both the cases the format got preserved and to achieve the above stated task we have encryption schemes like (FF3-1, FEA-1, and FEA-2) etc. and since each encryption algorithm needs a cryptanalysis to find the vulnerabilities or loopholes in the algorithm, there came linear cryptanalysis.

In cryptography we use two types of analysis schemes one is Linear cryptanalysis and another is Differential cryptanalysis, both the techiniques are used to attack the block / stream ciphers and linear cryptanalysis is one of the popular and used attacks on block ciphers. In the project we would be analyzing and studying linear cryptanalysis and format preserving encryption schemes in much more details and at the end some implementation regarding the encryption schemes and analysis can be expected.