Задача - зашифровать цифровую фотографию (для простоты можно ч/б) с помощью SP-сети (не путать SP-сеть с сетью Фейстеля)

Размер изображения — 512\*512 пикселей. При шифровании изображение разбивается на блоки, кратные одному байту. Затем блоки шифруются, а после этого, естественно, и расшифровываются (причем, должны расшифровываться правильно).

Выбирать размер шифруемого блока шифруемых данных в диапазоне 16 - 64 бита. Поскольку исходное изображение – черно/белое, то для отображения яркости пикселя изображения выделяется один байт. Исходя из сказанного, надо построить структуру своей SP-сети: задать для каждого раунда свой набор S-блоков и свой Р-блок. Описать и нарисовать структуру SP-сети. Привести построенные таблицы прямой подстановки (S-блоки) и Р-блок хотя бы для одного раунда шифрования. Далее надо выполнить один раунд шифрования, построить изображение, визуально оценить «степень его похожести» на шум. Для шумоподобного ч/б цифрового изображения характерно равномерное и хаотическое расположение точек в диапазоне яркостей от 0 до 255.

Для большей объективности целесообразно количественно оценить качество шифрования. Для этого есть простейший метод: надо построить гистограмму распределения яркостей изображения. Обычно одного раунда шифрования совершенно недостаточно для закрытия информации от посторонних. Поэтому их надо выполнить соответствующее количество, строя для каждого раунда свою «картинку» и свою гистограмму. Далее - дешифрование. Здесь надо привести таблицы обратной подстановки и т.д. в обратном порядке. Выводы о проделанной работе.

Можно выполнить в любой среде. Но должны быть представлены все необходимые промежуточные и т.д. результаты