Задание по проведению линейного криптоанализа шифра, основанного на структуре SPN

Требования

Провести линейный криптоанализ шифра с вашими вариантами таблиц замен и перестановок с целью определения от 8 и более бит пятого раундового подключа. Варианты указаны в приложении. Оформить полученные результаты в виде отчета.

В отчете:

1. привести таблицу замен и таблицу перестановок для вашего варианта;
2. привести таблицу линейных приближений блока замены для своего варианта (как в табл.4 документа «Линейный криптоанализ»);
3. показать, как рассчитываются значения в этой таблице на примере случайной величины с максимальным отклонением (как на рис. 4 документа «Линейный криптоанализ»);
4. построить линейное приближение шифра для своего варианта (вывод формульных соотношений). Показать графически как на рис. 5 документа «Линейный криптоанализ»;
5. привести фрагменты кода программы, которые были изменены для выполнения криптоанализа по вашему варианту;
6. вставить скриншоты результатов работы программы.
7. сделать вывод по итогам проведения линейного криптоанализа

Приложение. Варианты

(Sn, S – означает таблицу замен, n – номер варианта; Pn, P – означает таблицу перестановок, n – номер варианта; номер варианта соответствует номеру студента в списке группы)

S1=[3, 2, 6, 4, 7, 10, 8, 5, 11, 12, 13, 9, 15, 0, 1, 14]

P1=[8, 15, 10, 4, 7, 12, 13, 5, 11, 3, 0, 9, 14, 2, 6, 1]

S2=[3, 8, 13, 4, 14, 9, 10, 12, 5, 6, 0, 1, 11, 2, 7, 15]

P2=[2, 5, 6, 8, 4, 14, 0, 7, 11, 10, 12, 1, 15, 9, 3, 13]

S3=[12, 1, 9, 0, 10, 8, 3, 7, 13, 6, 11, 5, 15, 14, 2, 4]

P3=[5, 11, 1, 13, 2, 15, 0, 8, 3, 6, 12, 7, 9, 14, 4, 10]

S4=[0, 15, 9, 13, 11, 5, 7, 2, 12, 3, 8, 1, 6, 4, 14, 10]

P4=[12, 3, 1, 9, 15, 6, 0, 5, 10, 11, 8, 7, 2, 14, 4, 13]

S5=[6, 8, 13, 1, 5, 10, 2, 11, 15, 12, 9, 0, 14, 3, 7, 4]

P5=[4, 6, 3, 11, 7, 10, 15, 9, 14, 1, 2, 0, 8, 5, 12, 13]

S6=[6, 13, 2, 9, 15, 0, 8, 12, 14, 10, 4, 7, 11, 1, 3, 5]

P6=[4, 7, 9, 15, 12, 8, 3, 6, 11, 0, 5, 14, 1, 2, 10, 13]

S7=[0, 4, 1, 13, 6, 9, 5, 11, 12, 2, 15, 8, 14, 10, 3, 7]

P7=[15, 9, 0, 13, 11, 8, 1, 14, 4, 7, 3, 2, 10, 5, 6, 12]

S8=[4, 5, 7, 8, 2, 3, 12, 9, 15, 11, 1, 0, 14, 10, 13, 6]

P8=[4, 14, 0, 8, 10, 13, 5, 15, 6, 11, 2, 7, 9, 1, 12, 3]

S9=[10, 1, 0, 11, 6, 8, 5, 13, 3, 14, 2, 15, 7, 12, 9, 4]

P9=[3, 11, 10, 0, 5, 1, 13, 4, 8, 14, 2, 12, 6, 9, 7, 15]

S10=[6, 0, 3, 15, 10, 12, 13, 14, 7, 11, 5, 4, 9, 1, 8, 2]
P10=[14, 13, 0, 11, 2, 10, 4, 7, 12, 3, 1, 15, 8, 5, 6, 9]

S11=[2, 15, 0, 4, 5, 9, 8, 11, 6, 3, 14, 1, 13, 12, 10, 7]
P11=[9, 7, 2, 13, 15, 14, 11, 8, 3, 10, 0, 1, 4, 12, 6, 5]

S12=[10, 8, 13, 5, 1, 15, 3, 12, 7, 9, 11, 0, 4, 14, 6, 2]
P12=[9, 11, 4, 14, 0, 7, 5, 13, 15, 3, 1, 8, 12, 6, 10, 2]

S13=[15, 7, 10, 2, 13, 12, 0, 6, 3, 14, 9, 1, 11, 4, 5, 8]
P13=[7, 6, 3, 4, 5, 15, 10, 2, 11, 9, 0, 13, 12, 8, 14, 1]

S14=[2, 0, 7, 4, 6, 1, 12, 5, 13, 3, 14, 15, 8, 9, 11, 10]
P14=[2, 14, 0, 10, 3, 15, 13, 8, 12, 1, 7, 6, 5, 11, 4, 9]

S15=[8, 3, 5, 2, 15, 10, 4, 11, 0, 13, 12, 7, 9, 14, 1, 6]
P15=[8, 11, 5, 12, 9, 13, 1, 14, 6, 15, 4, 10, 3, 7, 2, 0]

S16=[8, 13, 0, 1, 5, 9, 10, 12, 15, 3, 2, 7, 11, 6, 14, 4]
P16=[4, 14, 15, 1, 11, 7, 12, 6, 13, 3, 9, 2, 0, 8, 5, 10]

S17=[6, 14, 1, 7, 11, 0, 4, 13, 8, 15, 9, 5, 2, 12, 10, 3]
P17=[6, 2, 14, 0, 8, 10, 11, 4, 9, 5, 3, 15, 7, 12, 1, 13]

S18=[12, 11, 7, 15, 6, 2, 1, 13, 14, 8, 0, 10, 4, 5, 3, 9]
P18=[7, 4, 2, 6, 15, 5, 0, 10, 8, 11, 3, 14, 12, 13, 9, 1]

S19=[6, 2, 12, 3, 1, 7, 0, 15, 4, 10, 14, 9, 5, 8, 13, 11]

P19=[6, 11, 13, 3, 9, 10, 14, 7, 15, 2, 1, 8, 4, 12, 0, 5]

S20=[0, 5, 9, 8, 4, 6, 14, 2, 1, 3, 7, 11, 13, 10, 12, 15]
P20=[5, 0, 3, 7, 15, 12, 2, 6, 13, 9, 11, 1, 10, 8, 14, 4]

S21=[6, 3, 15, 10, 0, 4, 2, 12, 9, 5, 13, 8, 11, 7, 14, 1]
P21=[15, 14, 3, 7, 6, 11, 8, 0, 12, 10, 9, 5, 13, 4, 2, 1]

S22=[14, 3, 6, 11, 0, 1, 12, 15, 5, 9, 8, 7, 13, 4, 10, 2]
P22=[0, 9, 4, 15, 8, 5, 14, 12, 3, 11, 2, 1, 7, 13, 10, 6]

S23=[5, 13, 4, 15, 11, 2, 9, 8, 10, 12, 14, 7, 0, 6, 1, 3]
P23=[13, 2, 1, 10, 3, 5, 0, 14, 9, 7, 11, 4, 6, 8, 15, 12]

S24=[9, 12, 15, 1, 0, 2, 10, 8, 14, 7, 6, 3, 11, 13, 4, 5]
P24=[15, 8, 0, 13, 6, 5, 14, 9, 2, 11, 10, 3, 7, 12, 4, 1]