ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

**Федеральное государственное бюджетное образовательное**

**учреждение высшего образования**

**«Санкт-Петербургский государственный университет телекоммуникаций**

**им. проф. М. А. Бонч-Бруевича»**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Кафедра Защищенных систем связи

Дисциплина «Основы криптографии»

# Лабораторная работа № 8

**Дифференциальный криптоанализ блочного шифра**

**Вариант 4**

Выполнил студент: Громов А.А.

Группа: ИКТЗ-83

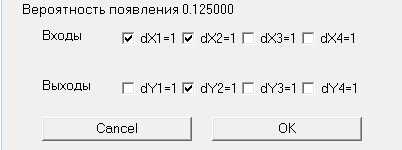
Профессор кафедры ЗСС: д.т.н. проф. Яковлев В.А.

**Цель работы:** Целью данной работы является изучение принципа дифференциального криптоанализа блочных шифров, реализованных по схеме SPN.

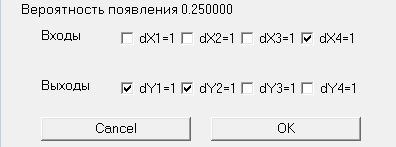
Ход выполнения работы:

Вероятности появления линейных комбинаций

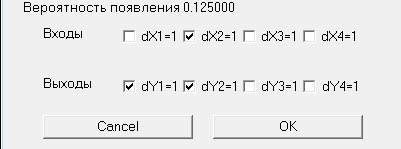
БЛОК S14



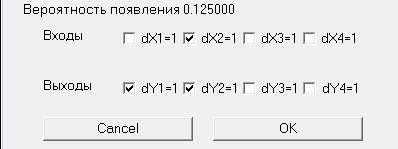
БЛОК S22



БЛОК S31



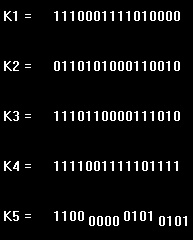
БЛОК S32



**Генерация ключа**

Выбран исходный ключ 1110001

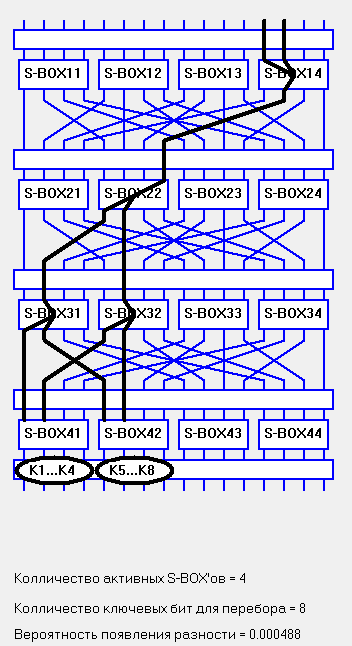
Раундовые ключи



Дифференциальный криптоанализ

|  |  |  |  |
| --- | --- | --- | --- |
| № варианта | 1 раунд | 2 раунд | 3 раунд |
| 4 | S14 | S22 | S31, S32 |

1. Сквозная дифференциальная характеристика



1. Скриншоты окна подбора ключа для разных N.

N=100



N=500



N=5000



1. Выводы:  
    Дифференциальный криптоанализ использует аномально повышенные вероятности появления некоторых разностей криптограмм для определенных разностей между открытыми сообщениями. Характеристикой сквозной дифференциальной характеристикой является вероятность пар разности S-блока в раундах. Они зависят от того, в каких S-блоках будем задавать сквозную дифференциальную характеристику. В лабораторной работе при расчете вероятностей по каждому раунду сделаем вывод, что в первом раунде вероятность максимальна, а во втором минимальна. Выбор истинного ключа производится исходя из 5 раундового ключа