МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний технічний університет України
«Київський політехнічний інститут»

РОЗДІЛИ СУЧАСНОЇ КРИПТОЛОГІЇ

Комп'ютерний практикум №2

Лінійний криптоаналіз блокових шифрів

Виконали:
студенти групи ФІ-73мп
Грубіян Євгеній
Свічкарьов Іван
Варіант – 4
Прийняв:
Деркач А.Г

Київ
2018

1. Мета роботи

Опанування сучасних методів криптоаналізу блокових шифрів, набуття навичок у дослідженні стійкості блокових шифрів до лінійного криптоаналізу.

2. Постановка задачі

1) 1

2) 2

3. Хід роботи

α \ β	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	0	2	0	2	0	2	0	0	2	2	0	0	2	2
2	0	0	2	0	0	0	0	2	0	0	2	0	2	2	2	4
3	0	0	2	2	2	2	0	0	2	0	0	2	2	0	0	2
4	0	2	2	2	2	0	0	0	2	2	0	2	0	0	2	0
5	0	4	2	0	2	0	2	2	2	0	0	0	0	0	0	2
6	0	0	0	4	2	0	0	2	0	0	0	0	4	2	2	0
7	0	0	0	2	0	0	2	0	2	2	0	2	0	4	0	2
8	0	0	0	0	0	2	0	2	2	2	2	2	2	0	2	0
9	0	2	0	0	0	2	4	0	0	0	0	2	2	2	2	0
A	0	0	2	2	0	4	2	2	0	4	0	0	0	0	0	0
B	0	0	2	2	2	0	2	0	0	2	2	0	4	0	0	0
C	0	2	0	0	2	2	0	2	0	4	2	0	0	2	0	0
D	0	0	0	0	2	0	2	0	2	0	2	0	0	0	4	4
E	0	0	2	0	2	0	2	2	0	0	2	4	0	2	0	0
F	0	4	2	0	0	2	0	0	4	0	2	0	0	2	0	0

Табл. 1: Таблиця диференціальних імовірностей 4-ого S-блоку $\times 2^4$

4. Висновки

1) 1

2) 2

3) 3

4) 4