МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний технічний університет України
“Київський політехнічний інститут”

РОЗДІЛИ СУЧАСНОЇ КРИПТОЛОГІЇ

Комп’ютерний практикум №1

Диференціальний криптоаналіз блокових шифрів

Виконали:
студенти групи ФІ-33
Грубіян Євгеній
Свічкарьов Іван
Варіант – 4
Прийняв:
Деркач .

Київ
2018

1. Мета роботи

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

2. Постановка задачі

1) Реалізувати пошук високоімовірних п'ятираундових диференціалів шифру Хейса методом «гілок та границь». Для пошуку рекомендується використовувати початкові різниці α із однією ненульовою тетрадою (це дає змогу максимізувати імовірності на перших етапах пошуку). Якщо у вихідній різниці будуть наявні нульові тетради, це може ускладнити проведення атаки: окремі біти ключа можуть не відновитись через брак статистичної інформації.

2) Реалізувати атаку на сьомий раундовий ключ шифру Хейса. Для побудови атаки використати знайдені на попередньому кроці диференціали із високою імовірністю.

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

Пошук високоімовірних диференціалів відбувався за методов «гілок та границь». Для прискорення пошуку були обрані такі порогові значення для імовірностей раундових диференціалів : $\{0.124, 0.00195, 0.0003, 0.00005, 0.00005\}$.

Початкові різниці α обиралися із однією ненульовою тетрадою, а вихідні різниці відбиралися із відсутніми нульовими тетрадами. Загалом, щоб атака була успішною з високою імовірністю, можна взяти 3 самі імовірні диференціали із зазначеними α у таблиці 2, використовуючи 16000 текстів. Щоб атака була успішною для деякого окремого диференцілу треба взяти $\frac{16}{p}$ текстів, де p – імовірність відповідного диференціалу. Формат таблиці 2 – імовірність|кількість співпадінь β із обрахунковою різницею пари текстів, розшифрованих на

α \ β	1111	2222	4264	4444	8888
0003		337|40|1,42			138 | 22 | 1,66
0005		294|24|1,71			133 | 14 | 1,40
0006		**681|38|1,46**			**286 | 36 | 2,25**
0009		**493|40|2,00**			209|24|2,00
000B		**424|46|1,64**			165|32|1,60
000D		**273|30|2,14**			103|16|1,60
0600	**454|26|1,30**				
6000	**375|36|2,00**		**342|16|1,14**	**711|22|1,83**	
9000	**260|22|2,20**			530|12|1,20	
B000	**234|28|2,33**		209|16|1,60	471|20|1,43	
D000			**307|34|2,42**		

Табл. 2: Таблиця диференціальній імовірностей, 10^{-6}

один раунд|у скількі разів ключ домінує над іншими. Другий, та третій параметр зазначені чисто для того, щоб подивитися, яка доля співпадінь може припадати на бажаний ключ.

Гарні початкові різниці $\alpha = \{0006{,}6000\}$, які обираючи саму імовірну вихідну різницю β, дають за 16000 текстів, бажаний сьомий раундовий ключ $k_7 = dea7$.

4. Висновки