**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) Реалізувати методом «гілок та границь» пошук п'ятираундових лінійних апроксимацій шифру Хейса із великим потенціалом.

2) Реалізувати атаку на перший раундовий ключ шифру Хейса.

# 3. Хід роботи

Пошук п'ятираундових лінійних апроксимацій шифру Хейса із великим потенціалом відбувався за методов «гілок та границь». Для прискорення пошуку були обрані такі порогові значення для раундових списків потенціалів : $\{0.00015, 0.00015, 0.00015, 0.00015, 0.000015\}$.

Початкові різниці $\alpha$ обиралися із однією ненульовою тетрадою.

Для успішної атаки треба було накопичити необхідну кількість $N$ пар «відкритий текст-шифротекст» ($X_0$,$X_r$) та – $M$ апроксимацій.

Ключ однозначно знаходився при:

1) $N = 8000, M = 300$, а лічильник ключа переходу через поріг $u = 0.7 \cdot \hat{u}_{max}(k)$, де

$$\hat{u}(k) = |\#\{(x,y) : \alpha \cdot X_1 \oplus \beta \cdot X_r = 0\} - \#\{(x,y) : \alpha \cdot X_1 \oplus \beta X_r = 1\}|$$

   був у 2 рази більше за другий у вихідному списку кандидатів у ключ.

2) $N = 4000, M = 1000$, а лічильник переходу через поріг $u = 0.7 \cdot \hat{u}_{max}(k)$ був на 14% більше за другий у вихідному списку кандидатів у ключ.

3) $N = 4000, M = 300$ – ключ був третім у списку кандидатів.

# 4. Висновки

- Від обраних параметрів $M$,$N$,$u$ залежить однозначне знаходження ключа.
- Було знайдено ключ: $k_0 =$ 0x3937 із використання 8000 пар текстів та 300 апроксимацій.