НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. СІКОРСЬКОГО»

НН ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4 З ПРЕДМЕТУ «СИМЕТРИЧНА КРИПТОГРАФІЯ»

«ПОБУДОВА ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ЛІНІЙНИХ РЕГІСТРАХ ЗСУВУ (ГЕНЕРАТОРА ДЖИФФІ) ТА ЙОГО КОРЕЛЯЦІЙНИЙ КРИПТОАНАЛІЗ»

Виконали:

ФІ-04 Коваль Марія

ФІ-04 Недашківський Іван

Перевіряв:

Чорний О.М.

Мета комп`ютерного практикуму

Ознайомлення з деякими принципами побудови криптосистем на лінійних регістрах зсуву; практичне освоєння програмної реалізації лінійних регістрів зсуву (ЛРЗ); ознайомлення з методом кореляційного аналізу криптосистем на прикладі генератора Джиффі.

Постановка задачі та варіант завдання

Характеристичні многочлени:

- для L_1: $p(x) = x^{30} \oplus x^6 \oplus x^4 \oplus x \oplus 1$, що відповідає співвідношенню між членами послідовності $x_{i+30} = x_i \oplus x_{i+1} \oplus x_{i+4} \oplus x_{i+6}$;
- для L_2: $p(x) = x^{31} \oplus x^3 \oplus 1$, відповідна рекурента: $y_{i+31} = y_i \oplus y_{i+3}$;
- для L_3: $p(x) = x^{32} \oplus x^7 \oplus x^5 \oplus x^3 \oplus x^2 \oplus x \oplus 1$, відповідна рекурента:

$$s_{i+32} = s_i \oplus s_{i+1} \oplus s_{i+2} \oplus s_{i+3} \oplus s_{i+5} \oplus s_{i+7}.$$

Імовірність помилки першого роду $\alpha = 0{,}01$.

Послідовність (z_i) знаходиться у файлі `Crypto_CP4_variants_2018.txt` (обирайте послідовність відповідно до вашого варіанту).

Замість основного варіанту завдання ви можете обрати спрощений варіант завдання. У спрощених варіантах регістри генератору Джиффі визначаються такими характеристичними поліномами:

- для L_1: $p(x) = x^{25} \oplus x^3 \oplus 1$, що відповідає співвідношенню між членами послідовності $x_{i+25} = x_i \oplus x_{i+3}$;
- для L_2: $p(x) = x^{26} \oplus x^6 \oplus x^2 \oplus x \oplus 1$, відповідна рекурента:

$$y_{i+26} = y_i \oplus y_{i+1} \oplus y_{i+2} \oplus y_{i+6};$$

- для L_3: $p(x) = x^{27} \oplus x^5 \oplus x^2 \oplus x \oplus 1$, відповідна рекурента:

$$s_{i+27} = s_i \oplus s_{i+1} \oplus s_{i+2} \oplus s_{i+5}.$$

Варіант виконаної роботи - №7.

Хід роботи, опис труднощів, що виникали, та шляхів їх розв’язання

Початково хід роботи йшов виключно за планом. Ми написали за даними нам характеристичними многочленами роботу ЛРЗ для всіх трьох регістрів. За формулами з опису комп’ютерного практикуму ми знайшли значення порогу C для регістрів 1-2 та кількість знаків N вихідної послідовності через квантилі нормального розподілу. Потім, використовуючи розпаралелювання, ми окремо на різних потоках проробили процедуру відбору для L_1, L_2, щоб знайти кандидатів, у

яких статистика R задовольняла умові. На даному етапі і виникли труднощі, які неможливо було фізично подолати, маючи дані нам ресурси. Тоді як для другого регістру у нас було віднайдено лише 2 кандидати, а саме

[[0,1,1,0,1,0,0,1,1,1,1,1,0,1,0,1,1,1,0,1,1,0,0,1,0,0],

[1,1,0,0,1,1,0,0,1,0,0,1,0,1,1,1,0,1,0,0,1,1,0,1,0,0]]

для першого ж регістру кандидатів було далеко понад 1000, ось деякі з них:

[[0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0],

[0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1],

[1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1],

[0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0],

[1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0],

[0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1],

[0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0],

[1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1],

[0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0],

[0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0],

[0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0],

[1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0],

[0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1],

[0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0],

[1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0],

[0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0],

Це призвело до того, що на останньому кроці, коли ми прийшли до порівняння усіх можливих відібраних кандидатів, включно з третім регістром, ми отримали на перевірку 9991782360 потенційних кандидатів на вхідну послідовність. Щоб обробити таку кількість різних послідовностей з обраною реалізацією, необхідно було б витратити десятки годин активної роботи комп’ютера, що занадто затратно і за ресурсами і за часом. Через що, остаточний результат не був отриманий.

Висновки

Під час виконання практикуму ми попрацювали з лінійними регістрами зсуву, на прикладі генератора Джиффі ознайомились з методом кореляційного аналізу

криптосистем. За допомогою знань зі спеціальних розділів обчислювальної математики та математичної статистики, ми довели, що генератор Джиффі має свої недоліки, які доволі легко взламувати, якщо мати відповідну кількість машинного та часового ресурсу. На жаль, розмір нашого варіанту перевищив усі ліміти даних ресурсів, що призвело до унеможливлення нами остаточного завершення даного комп’ютерного практикуму.