Висновок

У роботі представлено задачу створення програмної системи для підвищення захищеності ресурсів локальної мережі від різного роду атак.

Список використаних джерел

1. Юдін О. К. Захист інформації в мережах передачі даних / О. К. Юдін, О.Г. Корченко, Г.Ф. Конахович. - Видавництво Інтерсервіс, 2009. -716 с.
2. Новіков О.М. Безпека інформаційно-комунікаційних систем / О.М. Новіков, М.В. Грайворонський. - Видавництво BHV, 2009. - 608 с.
3. Конахович Г. Ф. Защита информации в телекоммуникационных системах. - МК-Пресс, 2005. - 288 с.
4. Норткат С. Обнаружение нарушений безопасности в сетях / С. Норткат, Д. Новак. - Вильямс, 2003. - 448 с.

УДК 004.9

КРИТЕРІЙ ЕФЕКТИВНОСТІ ДЛЯ ВИЗНАЧЕННЯ СТІЙКОСТІ БЛОКОВИХ ШИФРІВ НА ОСНОВІ ВНЕСЕНИХ ЗМІН СТАТИСТИЧНИХ ХАРАКТЕРИСТИК ШИФРОВАНОГО ТЕКСТУ

Глухова О.В.[1)], Лозинський А.Я.[2)], Яремкевич Р.І.[3)], Ігнатович А.О.[4)]

Національний університет «Львівська політехніка»

[1)] бакалавр; [2), 3)] магістр; [4)]аспірант.

І. Постановка проблеми

Стійкість шифрів звичайно оцінюють за критерієм, який визначає необхідні ресурси для визначення типу шифру, визначення ключа і дешифрацію тексту. Деякі шифри дають велику кількість можливих варіантів ключів (наприклад – мільйони і десятки мільйонів варіантів). Якщо раніше такі кількості закривали будь-які перспективи роботи з такими шифрами, то зараз ситуація корінним чином змінилася. На сьогоднішній день таке питання вирішується масованими атаками з використанням великої кількості технічних і людських ресурсів. Відомо, що в багатьох країнах світу сформовані кібер-війська, які мають можливість масованими атаками з погодженими діапазонами дослідних процедур розкривати шифри, які мають мільйони варіантів можливих ключів. Такі кібер-війська сформовані в КНР, РФ, США, і т.д. Багато країн і не афішують такі питання, але зрозуміло, що в сучасних умовах вижити без серйозного інформаційного захисту просто неможливо.

ІІ. Мета роботи

В криптографії відомі тисячі шифрів, використовуються сотні сучасних комп'ютерних шифрів. Важливо скрити не тільки ключ, але і використаний метод шифрування. Такі підходи вимагають нові оціночні критерії нових методів шифрування. На сучасному етапі зрозуміло, що майже всі шифри можна розкрити – справа тільки в затрачених ресурсах і часі. Дуже важливим є маскування використаного методу шифрування. Це вже є елемент боротьби не з криптографами, а з кібер-військами, які за досить короткі терміни відкривають складні сучасні шифри (RSA, DES, AES, мережа Фейстеля і т.д.). Метою є пошук і оцінка ефективності шрифтів, в яких виконується як шифрування з допомогою сучасних шифрів, так і маскування використаних методів шифрування інформації.

ІІІ. Особливості реалізації

Розглянемо використання запропонованого критерію ефективності на основі шифру Хілла. Шифр Хілла з точки ефективності і надійності, якщо розглядати його як ручний шифр – він є досить трудомісткий і тому неефективний. Надійність цього шифру також має слабі місця. Спосіб шифрування на основі шифру Хілла – поліграмний блоковий шифр підстановки, заснований на лінійній алгебрі. Цей спосіб шифрування давав можливість зашифровувати більш ніж k символів за один цикл. Шифрування інформації відбувається наступним чином. Кожній букві відкритого тексту присвоюється число. Для латинського алфавіту часто використовується найпростіша схема: A = 0, B = 1, ..., Z = 25, але це не є істотною властивістю шифру. Блок з μ букв розглядається як μ-мірний вектор і множиться

на **μxμ** матрицю по модулю 26. (Якщо в якості підстави модуля використовується число більше 26, то можна використовувати іншу числову схему – крім букв в алфавіт включають розділові знаки.) Ключем для шифру Хілла є матриця, яка представляється словом, чи довільним набором букв. Для шифрування використовується числова квадратна матриця (3x3, 4x4, 5x5,...). Матриця повинна мати обернену матрицю, щоб була можлива операція розшифрування.

Розглянемо результати, як змінився частотний аналіз зашифрованого тексту завдяки модифікації ВТ перед шифруванням – методом використання маскуючих символів. Критерієм покращення стійкості блокового шифру, є середнє інтегральне відхилення. Визначити середнє інтегральне відхилення можна за допомогою формули (1).

$$\sigma = \left[\frac{1}{2} \sum_{i=1}^{n} \frac{(x_{i\max} - x_i)}{x_{i\max}} \right] * 100\% \qquad (1)$$

Чим менше середнє інтегральне відхилення - тим складніше знайти ключі і визначити тип блокового шифру.

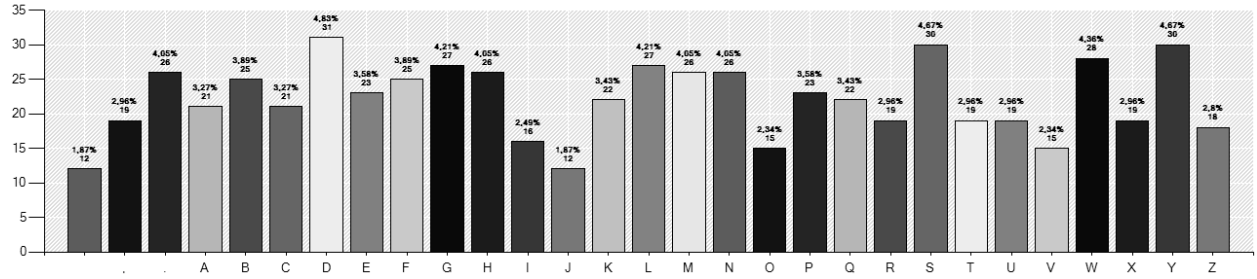

Рисунок 1 - Шифр Хілла (формат матриці ключа 3x3) без «маскуючих» символів.

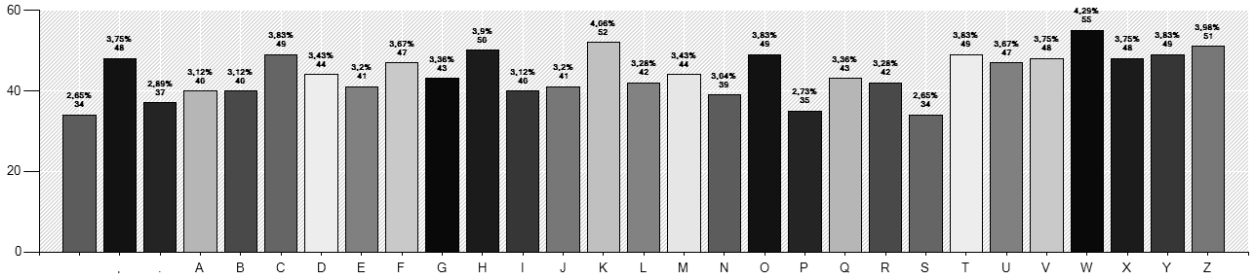

Рисунок 2 - Шифр Хілла (формат матриці ключа 3x3) з «маскуючими» символами.

Середнє інтегральне відхилення ШТ методом Хілла без «маскуючих» символів (рис. 3.9) рівне 27,3%, а ШТ з «маскуючими» символами (рис. 3.10) рівне 19,6%. Отже, завдяки модифікації ВТ покращено інтегральне відхилення у 1,4 рази для методу Хілла з маскуючими символами.

Але розшифрування ШТ, не маючи ключа, методом перебору всіх можливих варіантів ключа передбачає отримати ВТ який читається. Тому навіть якщо і зловмисники переберуть всі можливі варіанти ключа, усе одно не отримають ВТ який читається, оскільки відбувалася модифікація ВТ перед шифруванням. Вважаємо достатнім для ефективної зміни частотних характеристик забезпечити зменшення середнього інтегральне відхилення в 1,15-1,2 рази.

Висновок

Запропонований критерій визначення ефективності блокових шифрів на основі внесених змін статистичних характеристик шифрованого тексту дозволяє виконати кількісні оцінки внесених змін, які виконують різноманітні заходи. В основі сучасних підходів є така деформація статистичних характеристик шифрованих текстів, яка унеможливить виконати на основі частотного аналізу, і повторюваність блоків у зашифрованому тексті визначити тип шифра і підібрати для нього ключ.

Список використаних джерел

1. U.S. Patent 1 845 947. Лестер С. Хілл. Пристрій для шифрування. 1929.
2. Вербицький О.В. Вступ до криптології // Видавництво науково-технічної літератури. Львів, 1998. ISBN 966-7148-03-3.
3. Menezes A., van Oorshot P., Vanstone S. Handbook of applied cryptography. CRC Press, 1997.
4. Т.Коркішко, А.Мельник , В.Мельник. Алгоритми та процесори симетричного блокового шифрування – Львів, БаК, 2003.