УДК 681.3

А.О. ІГНАТОВИЧ
Національний університет "Львівська політехніка"

КРИТЕРІЙ ЕФЕКТИВНОСТІ ДЛЯ ВИЗНАЧЕННЯ СТІЙКОСТІ БЛОКОВИХ ШИФРІВ

Запропоновано критерій ефективності для визначення стійкості блокових шифрів на основі статистичних характеристик шифрованого тексту. Приведено результати дослідження найбільш поширених лінійних шифрів за розробленим критерієм ефективності. Запропоновано варіант покращення стійкості блокових шифрів.

Ключові слова: блокові шифри, стійкість шифру, критерій ефективності.

A.O. IHNATOVYCH
Lviv Polytechnic National University

EFFICIENCY CRITERION FOR DETERMINATION OF BLOCK CIPHER STRENGTH

Abstract- This research work proposes efficiency criterion for determination of block cipher strength. The introduced criterion is based on statistical characteristics of ciphertext. The results of the research of the most common linear ciphers using the introduced efficiency criteria are shown. Method of improvement of characteristics of block ciphers is proposed.

Keywords: block ciphers, cipher strength, efficiency criterion

Вступ

Стійкість шифрів, як правило, оцінюють за критерієм, який визначає необхідні ресурси для встановлення типу шифру та ключа, а також дешифрації тексту. Деякі шифри дають велику кількість можливих варіантів ключів, в окремих випадках – мільйони і десятки мільйонів варіантів. Якщо раніше така кількість варіантів фактично означала безперспективність роботи з такими шифрами, то зараз, внаслідок динамічного розвитку інформаційних технологій, ситуація докорінно змінилася. На сьогоднішній день питання взлому шифру вирішується масованими брутальними атаками з використанням великої кількості технічних і людських ресурсів. Відомо, що в ряді країн світу сформовані спеціалізовані підрозділи, які мають можливість масованими атаками з погодженими діапазонами дослідних процедур розкривати шифри, які мають мільйони варіантів можливих ключів. Такі спеціалізовані підрозділи сформовані у КНР, РФ, США, Англії, Франції, Німеччині. Ще цілий ряд країн не афішують інформацію щодо існування таких структур, але, зрозуміло, що неможливе функціонування інформаційних комплексів, які використовуються у різних сферах життя суспільства, без забезпечення серйозного інформаційного захисту. Тому дослідження у галузі засобів безпеки комп'ютерних систем та мереж, їх ефективності є актуальною задачею.

Огляд літературних джерел

У літературних джерелах достатня увага приділяється ефективності методів та алгоритмів шифрування інформації [1-6]. Водночас, відсутній простий критерій ефективності оцінки стійкості блокових шифрів.

Постановка задачі дослідження

Дослідити можливість застосування простого критерію ефективності оцінки стійкості блокових шифрів.

Основні результати дослідження

Однією із характеристик стійкості блокових шифрів є частота використання символів у шифрованому повідомленні. Пропонується використовувати як критерій оцінки стійкості блокового шифру середнє інтегральне відхилення.

Визначити середнє інтегральне відхилення можна за допомогою наступної формули:

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

де x_i, $x_{i\max}$ – кількість ***i***-х символів у шифрованому повідомленні та максимальне значення кількості символів відповідно; ***n*** – загальна кількість символів у алфавіті, що використовується у повідомленні.

Запропонований критерій ефективності інверсний. Що менше середнє інтегральне відхилення – то шифр ефективніший, то складніше знайти ключі і визначити тип блокового шифру.

Розглянемо особливості та результати застосування запропонованого критерію ефективності для деяких відомих шифрів і їх модифікацій. Досліджено та отримано результати, як змінився частотний аналіз зашифрованого тексту завдяки модифікації відкритого тексту (надалі – ВТ) перед шифруванням для всіх ступенів важливості інформації при застосуванні нового способу шифрування [7].

Середнє інтегральне відхилення шифрованого тексту (надалі – ШТ) методом Хілла без

“маскуючих” символів рівне 27,3% (рис. 1), а ШТ з “маскуючими” символами – рівне 19,6% (рис. 2). Отже, завдяки модифікації ВТ покращено стійкість у 1,4 рази для методу Хілла.

На усіх наведених рисунках по осі ординат вказана кількість ***i***-х символів у шифрованому повідомленні, що використовувалося при дослідженнях, та їх процентне співвідношення.

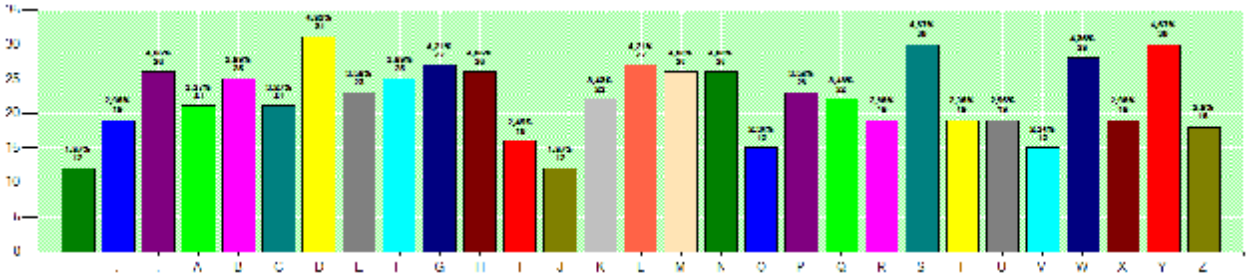

Рис. 1. Характеристика шифру Хілла (формат матриці ключа 3х3) без “маскуючих” символів

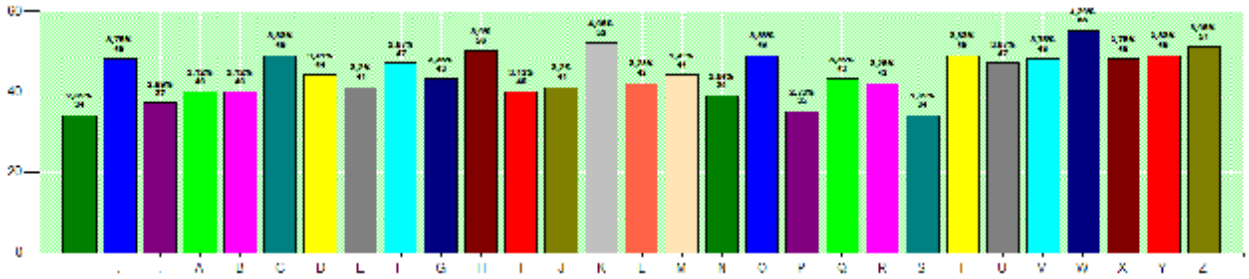

Рис. 2. Характеристика шифру Хілла (формат матриці ключа 3х3) з “маскуючими” символами

Середнє інтегральне відхилення ШТ методом Віженера без “маскуючи” символів рівне 57,3% (рис. 3), а ШТ з “маскуючими” символами рівне 41,2% (рис. 4). Отже, завдяки модифікації ВТ покращено стійкість у 1,4 рази для методу Віженера.

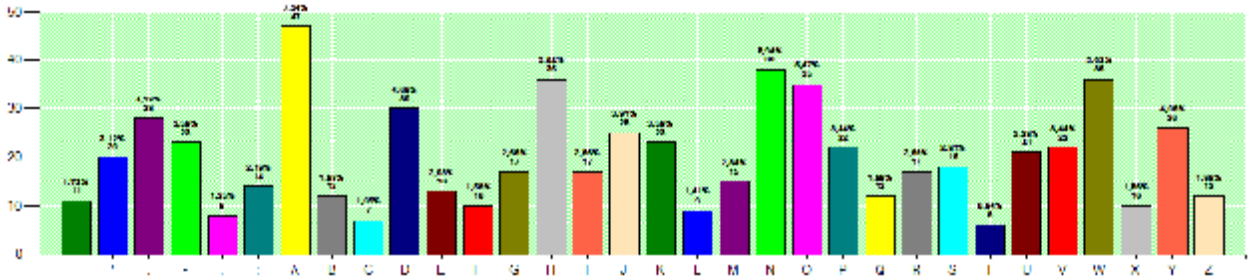

Рис. 3. Характеристика шифру Віженера без “маскуючих” символів

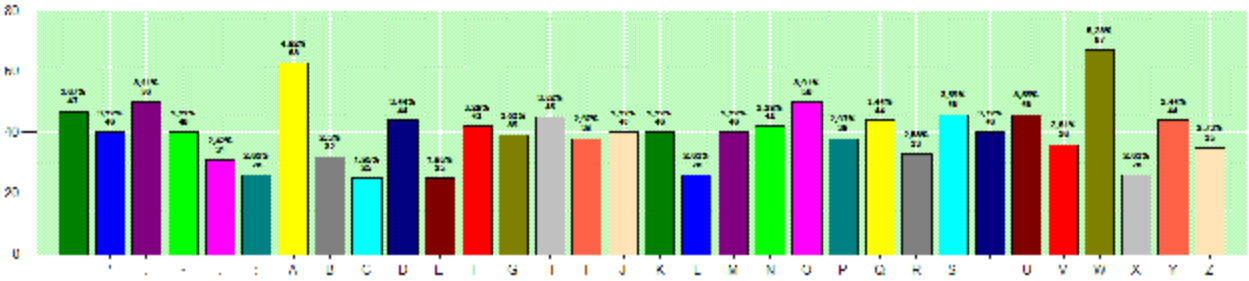

Рис. 4. Характеристика шифру Віженера з “маскуючими” символами

Середнє інтегральне відхилення ШТ методом Фейстеля без “маскуючи” символів рівне 68,2% (рис. 5), а ШТ з “маскуючими” символами рівне 58,9% (рис. 6). Отже, завдяки модифікації ВТ покращено стійкість у 1,2 рази для методу Фейстеля.

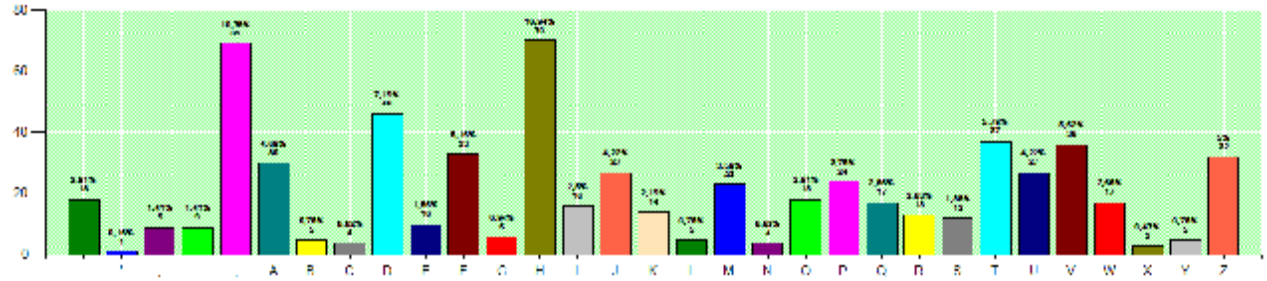

Рис. 5. Шифр Фейстеля без “маскуючих” символів

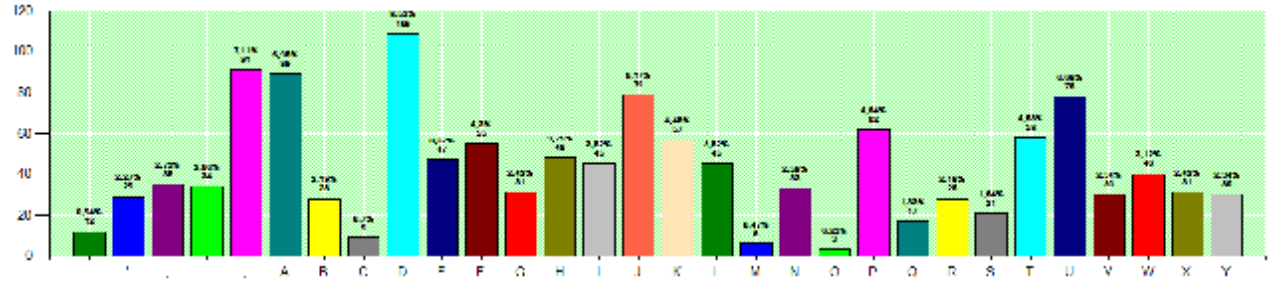

Рис. 6. Шифр Фейстеля з “маскуючими” символами

Середнє інтегральне відхилення ШТ методом Віженера + Фейстеля без “маскуючих” символів рівне 46,6% (рис. 7), а ШТ з “маскуючими” символами рівне 39% (рис. 8). Отже, завдяки модифікації ВТ покращено стійкість у 1,2 рази для методу Віженера + Фейстеля.

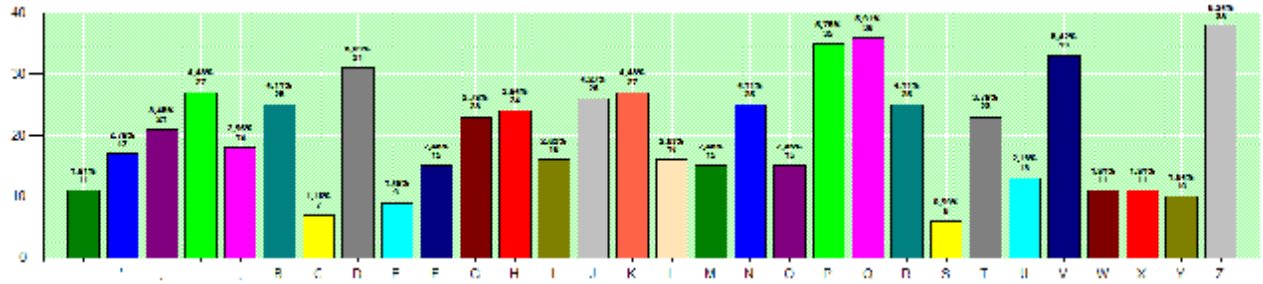

Рис. 7. Характеристика шифру Віженера + Фейстеля без “маскуючих” символів

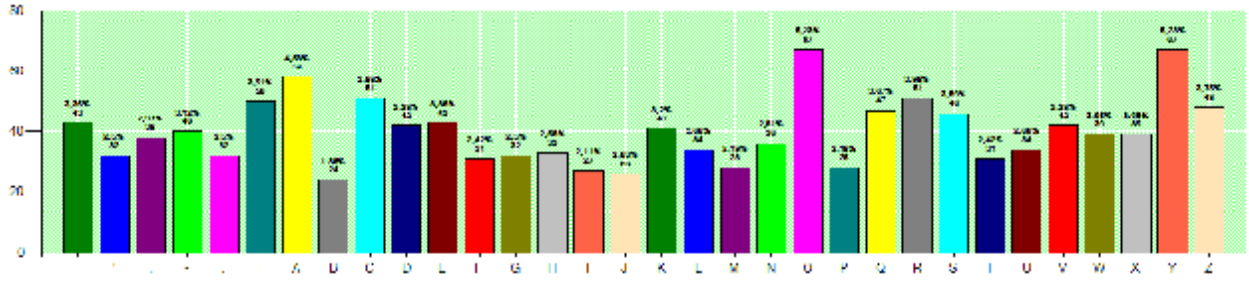

Рис. 8. Характеристика шифру Віженера + Фейстеля з “маскуючими” символами

Середнє інтегральне відхилення ШТ методом Хілла + Фейстеля без “маскуючих” символів рівне 40,8% (рис. 9), а ШТ з “маскуючими” символами рівне 17,6% (рис. 10). Отже, завдяки модифікації ВТ покращено стійкість у 2,3 рази для методу Хілла + Фейстеля.

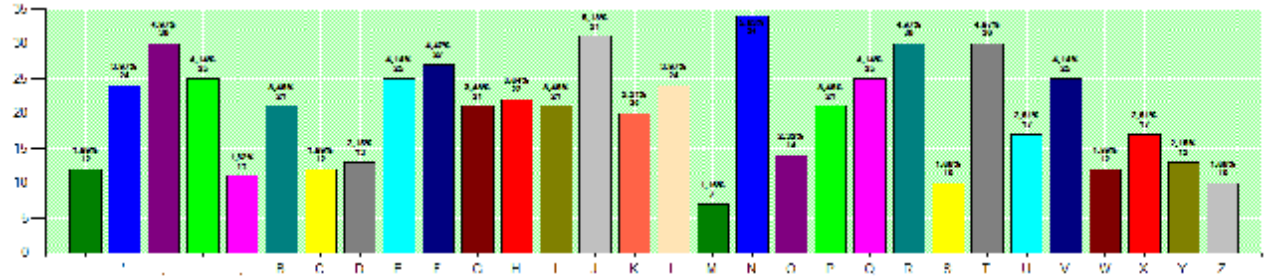

Рис. 9. Характеристика шифру Хілла + Фейстеля без “маскуючих” символів

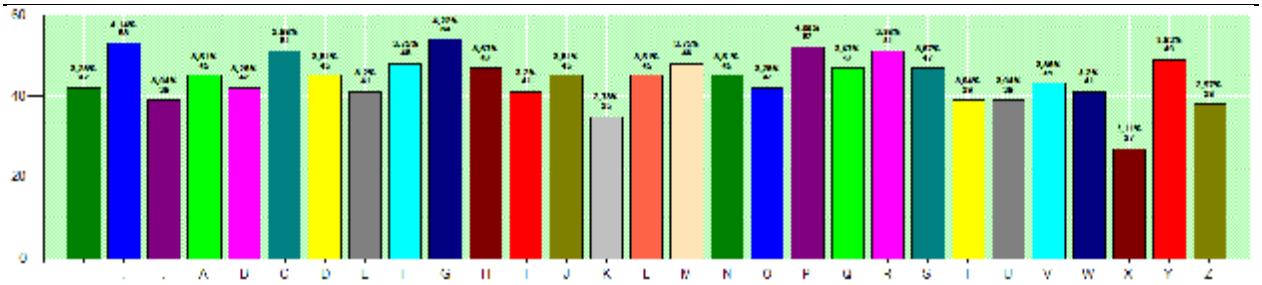

Рис.10. Характеристика шифру Хілла + Фейстеля з "маскуючими" символами

Модифікування ВТ для методів з використанням шифру Фейстеля не показує великої переваги. Але розшифрування ШТ методом Фейстеля, не маючи ключа, передбачає перебір всіх можливих варіантів ключа. Тому, навіть якщо і зловмисники переберуть всі можливі варіанти ключа, усе одно не отримають читабельний текст, оскільки відбувалася модифікація ВТ перед шифруванням.

Вважаємо достатнім для ефективної зміни частотних характеристик забезпечити зменшення середнього інтегрального відхилення в 1,15-1,2 рази. Ця величина визначається тим, що 15-20% зміни статистичних характеристик дезавуалює ті особливості ШТ, які допомагають визначити тип шифру, повторення в ШТ, які дозволяють визначити довжину ключа.

Нові комп'ютерні шифри можна будувати на комбінації шифрів і використанні маскуючих символів. Такі методи суттєво підвищують ефективність і надійність шифрування інформації.

Висновки

Запропонований критерій ефективності визначення стійкості блокових шифрів на основі статистичних характеристик шифрованого тексту дозволяє виконати кількісні оцінки ефективності, в тому числі внесених змін, які реалізовують різноманітні заходи шифрування.

Дослідження показали, що використання нових підходів шифрування дає можливість деформації статистичних характеристик шифрованих текстів, яка суттєво ускладнює визначення типу шифру та знаходження для нього ключа на основі частотного аналізу символів та повторюваності блоків у зашифрованому тексті .

Література

1. Fred Cohen . A Short History of Cryptography // Introductory Information Protection. — 1987. — ISBN 1-878109-05-7.

2. W. Stallings. Cryptography and network security. Principles and practice / William Stallings. – Pearson. – 2011. – 744 p.

3. Lester S. Hill . Cryptography in an Algebraic Alphabet». «The American Mathematical Monthly». – 1929.

4. U.S. Patent 1 845 947. Лестер С. Хилл. Пристрій для шифрування. 1929.

5. Ємець В. Сучасна криптографія: основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БАК, 2003. – 144 с.

6. Вербицький О.В. Вступ до криптології / О.В. Вербицький. – Львів: Вид–во науково-технічної літератури, 1998. – 248 с. –ISBN 966-7148-03-3.

7. Патент України на корисну модель № 99073, G 09C 1/00. Спосіб шифрування інформації / Ігнатович А.О., Іванців В. Р., Іванців Р-А. Д., Павич Н. Я. – u 201500619 ; заявл. 26.01.2015 ; опубл. 12.05.2015, Бюл. № 9.

References

1. Fred Cohen . A Short History of Cryptography // Introductory Information Protection. — 1987. — ISBN 1-878109-05-7.

2. W. Stallings. Cryptography and network security. Principles and practice / William Stallings. – Pearson. – 2011. – 744 p.

3. Lester S. Hill . Cryptography in an Algebraic Alphabet». «The American Mathematical Monthly».- 1929.

4. U.S. Patent 1 845 947. Lester S. Khyll. Prystriy dlya shyfruvannya. 1929. [in Russian]

5. Yemets' V. Suchasna kryptohrafiya: osnovni ponyattya /V. Yemets', A. Mel'nyk, R. Popovych. – Lviv: BAK. – 2003. – c. 144 [in Ukrainian]

6. Verbyts'kyy O.V. Vstup do kryptolohiyi // Vydavnytstvo naukovo-tekhnichnoyi literatury. Lviv, 1998. ISBN 966-7148-03-3. [in Ukrainian]

7. Ihnatovych A.O., Ivantsiv V. R., Ivantsiv R-A. D., Pavych N.Y. Sposib shyfruvannya informatsiyi. Patent Ukrayiny na korysnu model' #99073. Byul. #9 vid 12.05.2015. [in Ukrainian]

Рецензія/Peer review : 8.5.2015 р. Надрукована/Printed :15.5.2015 р.
Рецензент: д.т.н., проф., Наконечний А.Й.