УДК 004.056

РОЛЬ ОРГАНІЗАЦІЇ КЛЮЧА У ФОРМУВАННІ КРИПТОСТІЙКОСТІ КЛАСИЧНИХ МЕТОДІВ ШИФРУВАННЯ

Максим ГУМЕНЮК, Юрій СОЛОДЮК, Наталія МАСЛОВА, Орест ПОЛОТАЙ
Львівський державний університет безпеки життєдіяльності

Анотація. *Досліджено вплив організації ключа на криптостійкість класичних шифрів. Порівняння шифрів Цезаря та шифру Вернама показало, що стійкість визначається властивостями ключа — довжиною, випадковістю та одноразовістю застосування. Встановлено, що для шифру Цезаря модифікація алгоритму не усуває вразливості до криптоаналізу, тоді як шифр Вернама забезпечує інформаційно-теоретичну стійкість за умови використання випадкового одноразового ключа. Порушення цих вимог призводить до компрометації шифру.*
Ключові слова*: криптостійкість, шифр Цезаря, шифр Вернама, ключ, безпека даних.*

Abstract. *The study examines the impact of key organization on the cryptographic strength of classical ciphers. A comparison of the Caesar cipher and the Vernam cipher demonstrated that security is determined by the properties of the key — its length, randomness, and one-time use. It was established that modifying the Caesar cipher does not eliminate its vulnerability to cryptanalysis, whereas the Vernam cipher provides information-theoretic security only when a random one-time key is applied. Violation of these requirements leads to the compromise of the cipher.*
Keywords. *cryptographic strength, Caesar cipher, Vernam cipher, key, data security.*

У сучасній практиці інформаційної безпеки існує тенденція ототожнювати криптостійкість шифру з рівнем математичної складності алгоритму. Це призводить до ситуацій, коли шифрувальні системи, формально засновані на коректних криптографічних принципах, залишаються вразливими через недосконалі підходи до управління ключами: використання занадто коротких ключів, повторне застосування однакових ключів, детерміновані правила їх формування або передавання небезпечними каналами. У результаті криптоаналітичні атаки стають можливими не через слабкість алгоритму, а через неправильну організацію процесу ключового захисту. Ключ виступає центральним компонентом, що визначає межі криптостійкості шифру.

Актуальність. Дослідження впливу властивостей ключа на рівень захищеності є актуальним як з теоретичної, так і з прикладної позиції, оскільки навіть найпростіші математичні операції можуть забезпечити абсолютний рівень захисту за умови дотримання вимог до ключа.

Метою роботи є встановлення закономірностей між властивостями організації ключів (довжина, ентропія, одноразовість, спосіб застосування) та криптостійкістю класичних методів шифрування шляхом порівняльного аналізу зокрема шифру Цезаря та шифру Вернама.

Методика дослідження. Дослідження здійснювалось за такими показниками: довжина ключа, ентропія ключа, залежність ключа від структури алфавіту, та вплив повторного використання ключа на можливість відновлення відкритого тексту.

У шифрі Цезаря ключ є фіксованою константою (зсув по алфавіту), а його простір обмежений розміром алфавіту. Завдяки цьому криптоаналітик може передбачити межі можливих перетворень і виконати перебір ключів у скінченному діапазоні. Відомо [1], що статистичні характеристики мови у шифрі Цезаря не змінюються, що робить можливим застосування частотного аналізу без необхідності знати ключ. Таким чином, шифр Цезаря фактично не допускає зміни рівня криптостійкості через модифікацію ключа: навіть розширення алфавіту збільшує простір ключів лише лінійно, не впливаючи на структурну передбачуваність перетворень.

На відміну від інших класичних алгоритмів, криптостійкість шифру Вернама не є наслідком кількості або складності математичних операцій, а формується виключно властивостями ключа [2]. У випадку шифру Вернама (рис. 1), ключ — це послідовність випадкових елементів, довжина якої дорівнює довжині повідомлення. Стійкість алгоритму зростає разом із довжиною ключа і досягає максимально можливого рівня, коли ключ стає випадковим та рівним довжині повідомлення (рис. 2).

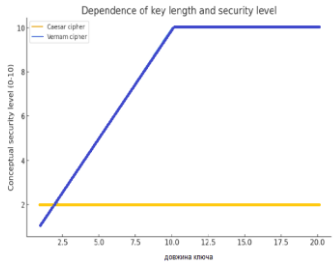

Рисунок 1 – Довжина ключа й стійкість алгоритмів

```python
def encrypt_decrypt_vernam(message, key):
    """
    Універсальна функція шифрування/розшифрування шифром Вернама (XOR).
    Працює з будь-яким Unicode-текстом.
    """
    #   Формуємо ключ до довжини повідомлення (або більше)
    key_stream = (key * (len(message) // len(key) + 1))[:len(message)]
    # XOR для кожного символу
    result = ''.join(chr(ord(m) ^ ord(k)) for m, k in zip(message, key_stream))
    return result


def generate_random_key(length):
    """
    Генерація криптографічно стійкого випадкового ключа.
    Повертає рядок символів (latin-1, бо 1 байт = 1 символ).
    """
    return secrets.token_bytes(length).decode('latin-1', errors='replace')
```

Рисунок 2 – Фрагмент програмного коду

Під час експериментальних обчислень підтверджено, що для випадкового і одноразового ключа неможливо отримати статистичний зв’язок між шифртекстом та відкритим текстом: для одного й того самого шифрте-

кcту, бо існує нескінченна кількість потенційних відкритих текстів, кожен із яких відповідає своєму можливому значенню ключа.

Показовими виявилися експериментальні випадки з повторним використанням ключа у шифрі Вернама. При повторі ключа з'являється залежність типу $C1 \oplus C2 = P1 \oplus P2$, яка є загрозою витоку інформації (C1, C2 – шифротекст, P1, P2 – відкриті повідомлення). Якщо при цьому хоча б частина одного з повідомлень стає відомою криптоаналітику, він може відновити ключ, а потім — всі повідомлення, у яких застосовано цей самий ключ. Таким чином, стійкість шифру Вернама є не властивістю алгоритму, а тільки наслідком правильної організації ключа: випадковість, довжина та одноразовість використання виступають необхідними та достатніми умовами. Структурний аналіз ключа продемонстрував, що саме ентропія ключа та відсутність повторів формують непередбачуваність алгоритму.

Зіставлення двох підходів показало, що структура алгоритму сама по собі не гарантує стійкість: у шифрі Цезаря збільшення складності трансформації не усуває передбачуваності, тоді як у шифрі Вернама одна й та сама операція XOR може забезпечити як повну стійкість, так і повну компрометацію залежно від режиму використання ключа.

Висновки. Шифр Цезаря та шифр Вернама належать до однієї історичної групи криптографічних алгоритмів (класичні), але демонструють різну стійкість в умовах зміни параметрів ключа. У дослідженні продемонстровано, що класичні шифри відображають два крайні сценарії: шифр Цезаря — приклад повної компрометованості методу через обмеження ключа, тоді як шифр Вернама — приклад абсолютної криптостійкості, досягнутої не ускладненням математичного перетворення, а коректною організацією ключа — випадковістю, довжиною та одноразовістю його використання. Таким чином, досліджені алгоритми шифрування демонструють різний рівень ефективності протидії криптоаналітичним атакам, але стійкість алгоритму ґрунтується не стільки на структурі шифрування, скільки на властивостях ключа, що контролює процес перетворення.

Література

1. Yarra Satya Sri Sowjanya, Nikitha Palakurthi, Punyamurthula V. Koushik, Marni Sriram, Vardhineedi Rajesh, N. Durga Deepti Priya. „Legacy Encryption: Unraveling the Caesar Cipher in Modern Data Security“ // International Journal of Scientific Research and Engineering Development. — 2025. — Vol. 8, Issue 2, March-April 2025. — С. 874-878. — URL: https://www.ijsred.com/volume8/issue2/IJSRED-V8I2P106.pdf

2. Kadum S. A. Developed OTP (One-Time Pad) Key Generation Method (2023) / S. A. Kadum // AIP Advances. — 2023. — Article No. 1823828. — DOI: https://doi.org/10.1063/5.0161788.