УДК 004.056.55

**І. О. Бондаренко**
**Т. М. Скидан**

# АТАКА «BRUTE FORCE» ТА СПОСОБИ ПІДВИЩЕННЯ СТІЙКОСТІ ШИФРІВ

Вінницький національний технічний університет

***Анотація***

*У статті розглянуто найбільш поширений вид атаки на шифр – brute force (або метод «повного перебору»). Проаналізовано його особливості та вразливості, а також описано способи підвищення стійкості шифрів до даної атаки.*

**Ключові слова:** криптографія, шифр, ключ, brute force.

***Abstract***

*The article provides the most common type of attack on a cipher - brute force (or the "full search" method). Its features and vulnerabilities were analyzed, as well as ways to increase the resistance of ciphers to this attack were described.*

**Keywords:** cryptography, cipher, key, brute force.

## Вступ

Станом на сьогоднішній день, в епоху високих технологій, безпека інформації стає ключовим питанням. Однією з найпоширеніших загроз є атака "brute force", що є практичної непроникною стратегією для зламування шифрів та отримання несанкціонованого доступу до конфіденційної інформації. У цьому контексті важливим стає розуміння принципів та методів, які можна використовувати для підвищення стійкості шифрів проти даної атаки.

## Результати дослідження

Метод грубої сили (англ. brute force), відомий також як метод повного перебору – найбільш поширений вид атаки на ключі шифрування. Він базується на систематичній перевірці усіх можливих варіантів ключів. Така атака може бути використана, коли неможливо скористатися іншими недоліками системи шифрування (якщо такі є), які полегшили б завдання [1].

Оцінка криптографічної стійкості шифрів базується на обчислювальній складності пошуку ключа шифрування методом повного перебору усіх можливих варіантів. Зокрема, шифр вважається криптостійким, якщо не існує методу "злому" значно швидшого, ніж brute force. Криптографічні атаки, засновані на методі повного пошуку, є найбільш універсальними, але й найбільш часозатратними [2].

Припустимо, що розмір ключа шифрування в бітах дорівнює b, відповідно, існує $2^b$ варіантів ключа. Для здійснення криптоаналізу та перевірки схильності до атаки, криптоаналітик повинен поступово перебрати усі можливі ключі, тобто застосувати в якості ключа шифрування значення 0, потім 1, 2, 3 і т.д. до максимально можливого ($2^b – 1$). У результаті ключ буде знайдений. Будь-який безпечний шифр повинен мати достатньо великий простір імовірних ключів, щоб запобігти цій атаці. В середньому, такий пошук вимагає $2^{b-1}$ тестових операцій шифрування [3]. Користувачі часто не використовують довгі ключі шифрування через складність їх запам’ятовування, однак чим коротшою є довжина ключа, тим більше він схильний до атаки шляхом повного перебору, що цілком під силу більшості сучасних комп’ютерів. Проте, при збільшені розрядності секретного ключа, наприклад, до 128-и біт, перебір стає менш можливим навіть для спеціальних обчислювальних систем [4].

Зрозуміло, що необхідно мати який-небудь критерій правильності знайденого ключа. У випадку атаки на основі відкритого тексту все просто – при тестуванні кожного ключа $K_x$ шифротекст C розшифровується і в результаті одержується певне значення M', яке порівнюється з відповідним йому відкритим текстом M. Збіг M = M' говорить про те, що шуканий ключ знайдений. Однак, із

атакою на основі шифротексту складніше. У цьому випадку необхідна наявність будь-якої додаткової інформації про відкритий текст, наприклад [3]:

1) У випадку, коли відкрите повідомлення є розбірливим текстом, написаним на будь-якій мові, то перехоплений шифротекст має мати достатній розмір для однозначного розшифрування. Мінімально достатній для цього розмір називається крапкою одиничності.

2) У випадку, коли відкрите повідомлення є бінарним кодом, необхідна яка-небудь інформація про те, що він із себе представляє. Якщо, наприклад, перехоплюється архів, то при переборі ключів кожне значення M' повинне розглядатися як можливий заголовок архіву. При іншому потенційному M це може бути PE-заголовок файлу, що використовується в Windows, заголовок графічного файлу і т.д.

Варто звернути увагу на те, що велика кількість засобів шифрування впроваджують у формат зашифрованого об'єкта контрольну суму відкритого тексту для перевірки його цілісності після розшифрування. Головне, що така контрольна сума може бути ідеальним еталоном, що цілком підходить для визначення вірного ключа і може бути використана зловмисником [3].

Існують декілька способів підвищення стійкості шифрів до атаки «brute force». Одним із них є обфускація (маскування) – спосіб захисту конфіденційної інформації від несанкціонованого доступу шляхом заміни вихідних даних фіктивними даними або довільними символами. Наступним способом є правильний вибір секретного ключа за наведеними вимогами [2]:

– ключ генерується індивідуально для кожного повідомлення (кожен ключ використовується лише один раз);

– ключ статистично надійний (тобто ймовірності кожного з можливих символів однакові, символи в послідовності ключів незалежні та випадкові);

– довжина ключа дорівнює або перевищує довжину повідомлення.

Підсумовуючи, варто зазначити, що достатньо надійним ключем шифрування вважається ключ довжиною не менше ніж 100 символів.

## Висновки

Отже, метод грубої сили (метод повного перебору) – це поширена атака на шифри. Розуміння методу грубої сили та принципів його дії є важливим для захисту зашифрованої інформації та забезпечення безпеки під час обміну конфіденційною інформацією. Описані способи підвищення стійкості шифрів до даної атаки, такі як обфускація, тобто ускладнення аналізу шифру шляхом використання додаткових алгоритмів чи прийомів, може допомогти ускладнити роботу зловмисникам, а правильний підбір секретного ключа є основою стійкості шифру до методу грубої сили.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Secret Double Octopus. Brute-force Attack. URL: https://doubleoctopus.com/security-wiki/threats-and-tools/brute-force-attack/

2. Тарнавський Ю. А. Технології захисту інформації : навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с.

3. Глинчук Л.Я. Криптологія: навч. посіб. Луцьк: СНУ ім. Лесі Українки, 2014. 186 с.

4. Жураковський Б. Ю., Недашківський О. Л. Система захисту інформації при передачі даних в радіоканалі: наук. роб. Київ: КПІ ім. Ігоря Сікорського, 2022. 34 с.

***Бондаренко Ірина Олексіївна*** **–** асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

***Скидан Тетяна Миколаївна*** **–** студентка групи УБ-21б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: tanaskidan1@gmail.com

***Bondarenko Iryna O.*** **–** assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua

***Skydan Tetyana Mykolaivna*** – student group SM-21b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: tanaskidan1@gmail.com