

ОСНОВНІ ТЕХНІКИ ШИФРУВАННЯ ДЛЯ ЗАХИСТУ ДАНИХ: ПОГЛИБЛЕНИЙ АНАЛІЗ ШИФРІВ ЦЕЗАРЯ, ТРАНСПОЗИЦІЇ ТА ВІЖЕНЕРА І ЇХ РОЛЬ У СУЧАСНІЙ КРИПТОГРАФІЇ

Пелюх О. І.¹; Михайловська О. В.²

^{1,2} Харківський національний університет імені В. Н. Каразіна

^{1,2} Україна, Харків

¹ oleksandr.peliukh@karazin.ua; ² olena.mykhailovska@student.karazin.ua

Анотація. У тезах розглянуто класичні методи шифрування: шифри Цезаря, транспозиції та Віженера. Проаналізовано їх переваги, недоліки та сучасне використання у криптографії. Обговорено концепції заміщення та транспозиції, що вплинули на розвиток сучасних алгоритмів шифрування. Зроблено висновок про значення цих методів і їх роль у забезпеченні інформаційної безпеки.

Ключові слова: криптографія; класичне шифрування; сучасні криптографічні матеріали.

Вступна частина. У сучасному цифровому просторі захист інформації від несанкціонованого доступу є важливим завданням як для урядів, так і для бізнесу та приватних осіб. Зростання кіберзагроз і випадків витоку даних призвело до того, що шифрування стало основою сучасної безпеки даних [1,2]. Техніки шифрування дозволяють перетворювати інформацію у незрозумілий формат, забезпечуючи, що лише авторизовані сторони можуть отримати доступ до цих даних. Нами досліджуються три основні техніки шифрування: шифр Цезаря, транспозиційний шифр і шифр Віженера. Хоча ці класичні шифри здаються базовими у порівнянні з сучасними криптографічними алгоритмами, вони відіграють важливу роль у розумінні основних принципів шифрування. Крім того, знання цих історичних методів дає змогу краще зрозуміти розвиток більш складних систем шифрування, що широко використовуються у сучасній практиці кібербезпеки [3]. Нами проаналізовано функціональність кожного методу, їхні сильні сторони та слабкості з погляду безпеки, а також їхню актуальність для сучасних технік шифрування.

Основна частина.

Шифр Цезаря є одним із найдавніших відомих методів шифрування, названий на честь Юлія Цезаря, який використовував його для захисту військових повідомлень [4]. Цей шифр належить до класу шифрів заміщення, в яких кожна літера відкритого тексту замінюється іншою літерою, зміщеною на певну кількість позицій у алфавіті. Принцип роботи такий:

$$C[i] = (P[i] + k) \bmod 26,$$

де:

$C[i]$ – зашифрована літера на позиції i ,

$P[i]$ – літера відкритого тексту на позиції i ,

k – значення зміщення (ключ),

26 – кількість літер в англійському алфавіті [1].

Наприклад, за зміщення на 3, відкритий текст HELLO перетворюється на:

$H \rightarrow K$

$E \rightarrow H$

$L \rightarrow O$

$L \rightarrow O$

$$O \rightarrow R$$

Отже, зашифрований текст – KHOOR.

Шифр Цезаря вразливий до частотного аналізу. Оскільки кожна літера зміщується на однакову кількість позицій, розподіл частот літер у зашифрованому тексті збігається з розподілом у відкритому тексті, що полегшує ідентифікацію найпоширеніших літер, таких як 'E' та 'A' [4]. Незважаючи на простоту, цей метод заклав основу для шифрів на основі заміщення та надихнув створення більш захищених шифрів.

Хоча сучасні методи шифрування значно еволюціонували, принцип зміщення символів у шифрі Цезаря був розширений у таких системах, як AES (Advanced Encryption Standard). У AES шари заміщення включають більш складні перетворення, що значно підвищує безпеку за рахунок додаткових елементів, таких як багаторівневі зміщення на основі ключів та нелінійні заміщення [5].

Шифр транспозиції відрізняється від шифру Цезаря тим, що в ньому переставляються (пермутація) символи відкритого тексту, а не замінюються іншими [2]. Це дозволяє зберігати літери незмінними, але змінювати їхній порядок у зашифрованому тексті. Принцип роботи такий:

$$C[i]=P[\pi(i)],$$

де:

P – відкритий текст,

π – функція пермутації, яка визначає порядок перестановки символів [3].

Розглянемо відкритий текст HELLO з ключем пермутації (3, 1, 4, 2, 5). Застосування цього ключа переміщує символи наступним чином:

- 1-ша літера (H) переміщується на 3-ю позицію,
- 2-га літера (E) переміщується на 1-шу позицію,
- 3-тя літера (L) переміщується на 4-ту позицію,
- 4-та літера (L) переміщується на 2-гу позицію,
- 5-та літера (O) залишається на 5-ій позиції.

Отже, зашифрований текст — LENLO.

Шифр транспозиції забезпечує більшу безпеку, ніж шифр Цезаря, оскільки частота появи літер зберігається, але їхній порядок приховується [6]. Однак, якщо ключ перестановки занадто короткий або передбачуваний, криптоаналітики можуть відновити оригінальне повідомлення, відгадуючи або реконструюючи ключ.

Техніки транспозиції є основоположними у сучасній криптографії, особливо в блочних шифрах, таких як DES та AES. У цих системах використовуються перестановки на рівні бітів для підвищення безпеки. Наприклад, DES виконує кілька раундів перестановок, щоб гарантувати, що навіть незначні зміни вхідних даних призведуть до значних відмінностей у зашифрованому тексті, що покращує стійкість до атак перебором.

Шифр Віженера будується на основі шифру Цезаря, використовуючи ключове слово для застосування різних зміщень до кожної літери відкритого тексту [5]. Такий підхід додає складності процесу шифрування і значно підвищує безпеку порівняно з простим шифром Цезаря. Розглянемо принцип роботи:

$$C[i]=(p[i]+K[i \bmod m])\bmod 26,$$

де:

K – ключове слово,

m – довжника K.

Наприклад, для шифртексту HELLO та ключового слова KEY, ключове слово повторюється відповідно до довжини тексту: KEYKE. Далі шифрування відбувається наступним чином:

$$\begin{aligned} H(7) + K(10) &\rightarrow R(17) \\ E(4) + E(4) &\rightarrow I(8) \\ L(11) + Y(24) &\rightarrow J(9) \\ L(11) + K(10) &\rightarrow V(21) \\ O(14) + E(4) &\rightarrow S(18) \end{aligned}$$

Отже, отриманий шифртекст – RIJVS.

Шифр Віженера значно безпечніший за шифр Цезаря, оскільки використання ключового слова змінює зміщення для кожної літери відкритого тексту. Це ускладнює криптоаналітичні атаки, зокрема частотний аналіз, оскільки кожна літера може шифруватися по-різному [7]. Однак шифр Віженера все ж залишається вразливим до атак за допомогою методів криптоаналізу з використанням повторюваних ключів (метод Касіскі), особливо якщо ключове слово є коротким або повторюється часто [8].

Ідея використання змінного ключа в шифрі Віженера має своє продовження в сучасних алгоритмах, таких як потокові шифри. Потокові шифри, як-от RC4, використовують змінні ключі для шифрування кожного біта або байта окремо, створюючи динамічний процес шифрування, що підвищує безпеку [6]. Крім того, принципи динамічного зміщення в шифрі Віженера стали основою для розробки більш складних систем, таких як одноразові блокноти (one-time pad), які забезпечують ідеальну криптографічну безпеку, коли використовуються одноразові випадкові ключі [5].

Шифр Цезаря, транспозиційний шифр і шифр Віженера є прикладами різних підходів до шифрування, кожен із яких має свої переваги та обмеження. В таблиці наведено ключові характеристики цих методів (табл. 1).

Таблиця 1 – Порівняння класичних шифрів

Шифр	Тип	Переваги	Недоліки	Використання в сучасній криптографії
Цезаря	Заміщення	Простота, легкість реалізації	Вразливість до частотного аналізу	Використовується для демонстрації базових принципів
Транспозиції	Перестановка	Збереження розподілу частот літер	Вразливість до атак на основі перестановок	Принцип використовується в блочних шифрах (AES)
Віженера	Поалфавітний	Захищеність від простого частотного аналізу	Вразливість до атак на повторювані ключі	Принципи динамічного ключа застосовуються в потокових шифрах

Кожен із цих шифрів є важливою ланкою в історії криптографії, демонструючи, як розвивалися методи захисту даних. Хоча сучасні алгоритми шифрування набагато складніші, основні концепції цих класичних шифрів залишаються актуальними й у сучасних системах безпеки [1, 2].

Шифри Цезаря, транспозиції та Віженера відіграли важливу роль у розвитку криптографії, закладаючи основу для складніших методів шифрування, що використовуються сьогодні. Сучасні криптографічні алгоритми, такі як AES, DES та RSA, інтегрують ідеї заміщення, транспозиції та використання змінних ключів, підвищуючи стійкість до атак і забезпечуючи високий рівень безпеки даних [5].

Наприклад, алгоритм AES, один із найпоширеніших симетричних шифрів, використовує багаторівневі заміщення та транспозиції для шифрування даних. Шифри заміщення, такі як шифр Цезаря, стали прототипом для процесів заміщення в AES, тоді як транспозиції використовуються для перемішування бітів даних, створюючи додатковий рівень захисту. Крім того, шифр Віженера надихнув на розробку поточкових шифрів, які застосовують змінні ключі для шифрування кожного біта або байта інформації [3].

Висновки. Шифри Цезаря, транспозиції та Віженера, незважаючи на свою простоту, залишаються важливими історичними прикладами криптографії. Вони не тільки заклали фундамент для сучасних методів шифрування, але й допомагають краще зрозуміти принципи, які лежать в основі сучасної криптографічної безпеки. Хоча ці шифри самі по собі більше не використовуються для забезпечення захисту даних, їхній вплив на розвиток сучасних алгоритмів, таких як AES та поточкові шифри, очевидний. У сучасному світі кібербезпеки ці методи продовжують надихати на створення нових підходів до захисту інформації, роблячи внесок у безпеку нашого цифрового середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Kessler, G. C. (2017). *An overview of cryptography*.
- [2] Schneier, B. (1996). *Applied cryptography: Protocols, algorithms, and source code in C (2nd ed.)*.
- [3] Stallings, W. (2017). *Cryptography and network security: Principles and practice (7th ed.)*.
- [4] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*.
- [5] Katz, J., & Lindell, Y. (2020). *Introduction to modern cryptography (3rd ed.)*.
- [6] Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography engineering: Design principles and practical applications*.
- [7] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.
- [8] Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644-654.

Oleksandr Peliukh, Olena Mykhailovska

Fundamental Encryption Techniques for Data Security: An In-Depth Analysis of Caesar, Transposition, and Vigenère Ciphers and Their Relevance to Modern Cryptography

Abstract. *The thesis deals with the classical encryption methods: Caesar, transposition and Vigenère ciphers. Their advantages, disadvantages and modern use in cryptography are analysed. The concepts of substitution and transposition, which influenced the development of modern encryption algorithms, are discussed. A conclusion is made about the importance of these methods and their role in ensuring information security.*

Keywords: *Cryptography; Classical encryption; Modern cryptographic algorithms.*