УДК 004.056.53

В. О. Демченко
А.О. Лівандовська
В. С. Катаєв

ВІД ШИФРУ ВІЖЕНЕРА ДО «ЕНІГМИ»: ЕВОЛЮЦІЯ МЕТОДІВ ШИФРУВАННЯ

Вінницький національний технічний університет

Анотація

За ідею було взято одні із найвідоміших історичних методів шифрування: Віженер та машина «Енігма», які в свій час допомогли людям передавати засекречену інформацію і додатково зробили вагомий внесок у розвиток криптографії. Початок дослідження було розпочато з моменту потреби передавати інформацію без сторонніх осіб. Розглянуто та проаналізовано історію вдосконалення методів шифрування та знайдено відмінності, які подано за характеристикою переваг та недоліків.

Ключові слова: шифрування, метод шифрування машиною «Енігма», метод шифрування Віженера, криптографія, алгоритм, метод, комутаційна панель, ротори.

Abstract

The idea was based on some of the most famous historical encryption methods: The engineer and the Enigma machine, which in their time helped people transmit classified information and additionally made a significant co-ntribution to the development of cryptography. The study began with the need to transmit information without third parties. The history of encryption methods has been reviewed and analysed, and differences have been found , which are presented in terms of advantages and disadvantages.

Key words: encryption, Enigma encryption method, Vigenère encryption method, cryptography, algorithm, method, patch panel, rotors.

Вступ

Ми живемо у світі сучасних технологій, де захист інформації є однією із найважливіших складових. Саме тому розробка нових, складніших шифрів є передовим завданням людства, при чому цей процес у своєму розвитку вже пройшов певний історичний шлях. З часом можливих комбінацій ставало все більше і більше, тому навчатись на історичних шифрах та вдосконалювати їх – є невід'ємною роботою у створенні нового. Аналізуючи історію розробки шифрувань, потрібно виділити шифрування Віженера, яке було один із перших хто використовував ключ для ускладнення та забезпечення надійності захисту інформації, а також шифрування методом «Енігми» - вдосконалений шифр Віженера. І саме ця комбінація дала великий поштовх у криптографії, адже саме цей метод був основою початку та закінчення Другої світової війни.

Результати дослідження

Шифр Віженера шифрує кожну літеру вхідного тексту за допомогою ключового слова, літери вхідного тексту зсуваються на певну кількість позицій, за порядком символів ключа. Для шифрування повідомлення використовують таблицю Віженера або по іншому її називають квадрат Віженера. Це така таблиця, рядки якої складаються з літер алфавіту, де кожен рядок зсувається на одну позицію, тим самим формуються всі можливі зсуви літер. Для зашифрування повідомлення по-трібно знайти перетин відповідних літер вхідного тексту та ключа у квадраті Віженера, який визначає зашифровану літеру [1].

Одним із недоліків шифрування Віженера, є те що коли довжина вхідного повідомлення більше за довжину ключа, рішенням даної проблеми – дублювання ключа. З цього випливає, що цей метод шифрування є циклічним і саме це полегшує роботу для взламу його.

Перед початком Другої світової гостро стало питання передачі інформації у нечитабельному вигляді. Першими на практиці реалізували це німці, створивши машину Енігму, яка по суті була спадкоємцем шифрування Віженера, продовжували ускладнювати її протягом усього періоду війни.

Принцип її роботи такий [2]: є декілька роторів, клавіатура та екран із лампочками, які світились літерами латинського алфавіту. Згодом була додана ще комутаційна панель. На екрані оператору показувалася буква, якою шифрувалась натиснута літера на клавіатурі. Те, якою буде зашифрована літера, залежало від початкових конфігурацій роторів. При кожному натисканні на клавіатурі, ротори змінювали свої позиції по черзі. Першим повне коло проходив правий ротор, потім той що по центру і останній – лівий. З додаванням комутаційної панелі, літера могла змінитись ще два рази. Таким чином існувало понад декілька трильйонів можливих комбінацій, що і робило злам машини най-важчим завданням 20 століття. Проте недоліком було неможливість зашифрувати літеру саму в себе, що і призвело до спрощення та зламу машини.

Шифрування Віженера можна подати нестандартним виглядом, наприклад: дві «двадцятишестишестерні» (якщо використовувати латинський алфавіт), з'єднавши їх паралельно одна до одної. Перша буде символізувати вхідне повідомлення і буде нерухомою, а друга буде символізувати вихідне повідомлення, яке ми будемо крутити відповідно до ключа, це буде так званий пристрій Віженера.

Шифрування машиною «Енігма» відбувається за допомогою роторів, а ротор це вищеописаний механізм, але з'єднання «двадцятишестишестернів» відбувається в «хаотичному» порядку та ключ – алфавіт, який починається з виставленої літери та змінюється після кожного натискання. І таких роторів від 3 до 5 в залежності від моделі Енігми.

Отже ми бачимо подібності між двома методами, а їх відмінності наведено у таблиці 1.

Таблиця 1 – Відмінності у методі шифрування Віженера та машини «Енігми.»

Ознака	**Шифрування Віженера**	**Шифрування машиною «Енігма»**
Шифрування	Можливе ручне шифрування	Потребує спеціального пристрою
Ключ	Відносно короткий	Складна комбінація
Недолік	Періодичність ключа та неможливість зашифрувати літеру саму в себе (за винятком літери «А»)	Неможливість зашифрувати літеру саму в себе
Метод шифрування	Статичний (ключ один і той самий)	Динамічний (ключ змінюється кожного разу)
Принцип роботи	Простий по алфавітний зсув	Комбінація електричних сигналів і механіки

Обидва методи шифрування були найскладнішими в свої часи і давали поштовх новим ідеям, адже вони не були схожі ні на що інше.

Висновки

Проаналізувавши все вище сказане, можна зробити висновок, що еволюція в методах шифрування справді існує. Шифрування Віженера та машиною Енігми ґрунтуються на багатоалфавітному шифруванні задля забезпечення конфіденційності. Але головний недолік Віженера – повторюваність ключа, був усунений у машині «Енігми» через *чотири* століття. Проте вона успадкувала недолік від попереднього методу шифрування, який не змогли усунути, що і спричинило її злам, неможливість зашифрувати літеру саму в себе. Недоліки в кожному методі шифруванні давали можливість наступному поколінню проаналізувати помилки минулого та вдосконалити свої методи чим і займають теперішні фахівці в сфері криптографії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Шифрування та дешифрування шифром Цезаря, Вернама , Віженера. URL: https://teteryakv12.wordpress-.com/2014/10/07 (дата звернення: 14.04.25).
2. Німецька "Енігма": легендарна машина, яка змінила хід Другої світової URL: https://24tv.ua/nimetska_enigma_legendarna_mashina_yaka_zminila_hid_drugoyi_svitovoyi_n1273305 (дата звернення: 14.04.2025).

Лівандовська Анастасія Олегівна – студентка групи 1БКС-23Б, Факультет інформаційних технологій комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, anastasialivandovska@gmail.com

Демченко Вероніка Олександрівна – студентка групи 1БКС-23Б, Факультет інформаційних технологій комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, vdemcenko234@gmail.com

Науковий керівник: ***Катаєв Віталій Сергійович*** – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, kataev@vntu.net.

Anastasiia Livandovska – student of group 1BKS - 23B, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: anastasialivandovska@gmail.com

Veronika Demchenko – student of group 1BKS - 23B, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vdemcenko234@gmail.com

Vitaliy Kataiev – assistant of the Department of Management and Security of Information Systems; Vinny-tsia National Technical University , Vinnytsia, kataev@vntu.net