УДК 004.415.3

МОДЕЛЬ ЕЛЕКТРОМЕХАНІЧНОЇ ШИФРУВАЛЬНОЇ МАШИНИ ЕНІГМА

MODEL OF ELECTROMECHANICAL ENCRYPTION MACHINE ENIGMA

Микола Головін, Ніна Головіна, Дмитро Гузачов

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *A visual model of encryption and decryption with the Enigma code using ordinary two-dimensional tables is presented. This original visual application can be used when studying a related topic in data encryption. The presented visual model can also be interesting as a conceptual precursor to a software implementation of the Enigma electromechanical encryption machine model in a university cryptography or programming course.*

Електромеханічна шифрувальна машина Енігма, як пристрій зіграла важливу роль в історії другої світової війни. Саме цією машиною шифрували свої повідомлення «вовчі зграї» німецьких підлодок, які у великій кількості топили військово-морські конвої з Америки в Европу. Злам коду Енігми дозволив у значній мірі покращити ситуацію в «битві за Атлантику» і в кінцевому рахунку виграти війну з нацистами. Ця боротьба у великій мірі стимулювала появу перших комп'ютерів. Задача шифрування та дешифрування кодом Енігми є цікавою задачею в університетському курсі криптографії. Ця ж задача цікава і в курсі програмування, при вивчені тем роботи з масивами, текстами і файлами.

Метою роботи є розгляд модельної реалізації електромеханічної шифрувальної машини Енігма за допомогою звичайних двомірних таблиць.

Принцип роботи машини Енігма був наступний. Шифрування здійснювалось трьома дисками. Кожен диск мав свій хаотичний порядок букв алфавіту. При проходжені електричного сигналу через три диски, на кожному буква міняла свій вигляд. Далі сигнал попадав на відбивач, де відбувалась своя заміна букви на букву. Після відбивача сигнал переплутування букв проходив через диски в зворотньому напрямку, де відбувались свої заміни. Машина була схожа на друкарську машинку. Натискування будь-якої клавіші приводило до прокручування першого диску на наступну букву тобто на 1/26 оберта. Обертались і інші два диски. Другий диск повертався на 1/26 оберта після повного оберта першого диску. Третій диск повертався на 1/26 після повного оберта другого диску [1].

Модельне представлення роботи Енігми (рис.1). Букви, що розташовані по ободах дисків представлені у вигляді рядків. Порядок букв у рядках зберігає порядок букв на ободах дисків. Також зберігається і взаємне розташування букв різних дисків (рядків). Букви дисків і відбивача виділені жирним. Обертання диску на одну позицію (1/26 оберту) виглядає як зникання одної букви з лівого краю рядка і додавання її з правого. Для зручної візуалізації електричних з'єднань та поворотів шифрувальних дисків біля дисків і відбивача написано реперний ряд букв в алфавітному порядку. Ці букви виділені нахилом.

У приведеному прикладі шифрується текст «HELLO WORLD». Результат шифрування «MZAGW LYDVZ». Шифрування перших трьох букв представлено на рис.1. Так перша буква при переході від диску до диску і при відбиванні отримує наступні значення **H=>F=>K=>D=>H=>T=>P=>M.** Еволюцію переходів можна відслідкувати за відповідним фоновим виділенням букв і стрілочками. Важливим моментом шифрування Енігми є обертання дисків при наборі тексту.

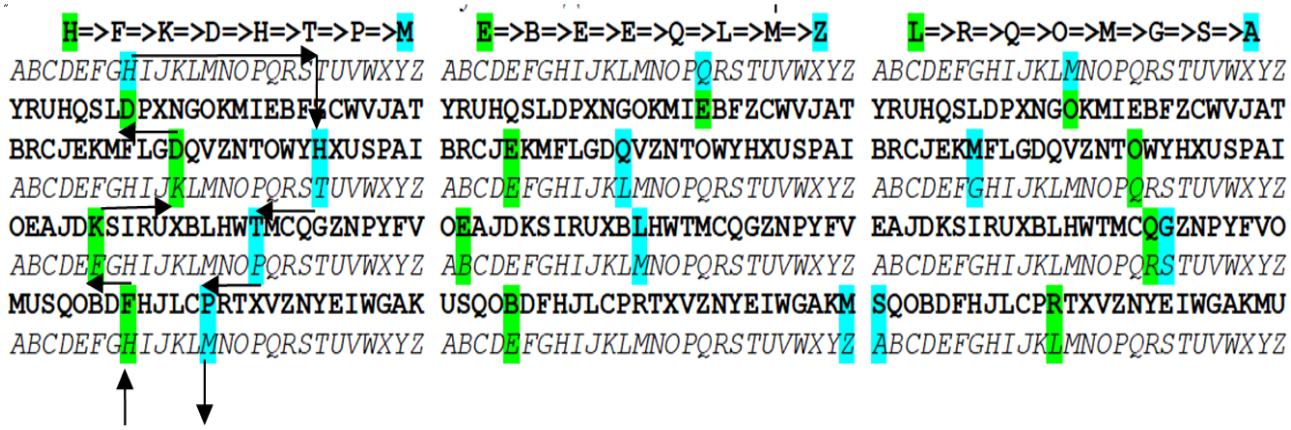

Рис.1 Схема шифрування Енігми букв: H в M, E в Z, L в A.

В прикладі текст короткий, тому можна бачити «обертання» тільки вхідного диску (нижній рядок). Ця обставина сильно ускладнює злам. Адже однакові букви тексту, що шифрується будуть виглядати, як різні, а різні, як однакові. Так буква «L» в тексті має в шифрограмі вигляд: «A», «G», «V», а букви «E» та «D» в тексті в шифрограмі виглядають, як «Z». Представлена наочна модель важлива, як понятійна предтечія програмної реалізація Енігми в курсі криптографії або програмування.

Бібліографія

1. F.L. Bauer. Decrypted Secrets: Methods and Maxims of Cryptology. 4th edition. Springer:, 2006. 539 p.