УДК 368.016

С.П. Рендюк, к.пед. н.,доцент,
І.В. Рассоха, к.ф.-м. н.,доцент,
З.С. Карнаух, учень ПМ-33,ПМБЛ №1 ім. І.П. Котляревського,
Д.О. Глушак, студент гр.102-ТН,
І.Ю. Закаблук, студент гр. 103-ТН.
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ОСНОВНІ МЕТОДИ ШИФРУВАННЯ ТА ДЕШИФРУВАННЯ ІНФОРМАЦІЇ: ІСТОРИЧНІ АСПЕКТИ

Як відомо, математичні методи є потужними засобами багатьох точних та технічних наук. Тому вивчення основних та прикладних розділів математики є невід'ємною частиною освіти сучасного інженера. Яскравим прикладом такого застосування є криптологія, більшість засобів якої базується на знаннях з вищої або прикладної математики. Тому вивчення історичних аспектів даної науки в розрізі математичних методів, які там використовуються є потужнім засобом формування математичної та професійної компетенції інженера.

Розглянемо еволюцію основних методів шифрування та дешифрування інформації вздовж століть, їх удосконалення. Майже чотири тисячі років тому в місті Менет-Хуфу на березі Нілу невідомий єгипетський переписувач намалював ієрогліфи, що розповіли історію життя його пана. Цей напис дійшов до наших днів та був вирізаний приблизно в 1900 році до н.е. на гробниці знатної людини на ім'я Хнумхотеп. Зробивши це, невідомий єгиптянин став родоначальником документально зафіксованої історії криптографії. Однак ці ієрогліфи все ж таки не були тайнописом у тому значенні, як його розуміють сьогодні. Одним з найдавніших шифрів який знайшли археологи вважається так званий «шифр Цезаря». Але якщо співставити кожному символу абетки його порядковий номер, то таке шифрування та дешифрування можна виразити формулами модульної арифметики. Тому можна вважати цей шифр одним із перших, що правда несвідомо, але використав у собі математичні методи теорії подільності [1].

В XVII-XVIII століттях стає все більш зрозуміло, що захист інформації - не стільки мистецтво твору й відгадування витончених шифрів, скільки точна наука. Усе помітніше перехід криптографії з області чорної магії в область чистої математики. Ми майже нічого не знаємо про те, чи займалися провідні математики того часу проблемами шифрування й дешифрування, але є дані, що деякі з них володіли криптографією. Серед них Блез Паскаль, що зробив ряд відкриттів в області комбінаторики й метод, що створив, індуктивного доказу; Ісаак Ньютон і Готфрид Лейбніц, що розробили диференціальне й інтегральне числення. Відомий

англійський філософ Ф. Бекон запропонував ідею двійкового кодування. Леонард Ейлер вів великі дослідження з перерахування й побудови латинських квадратів, тобто шифрів заміни. Математик Франсуа Вієт, будучи молодим офіцером розвідки, знайшов ключ до шифру іспанського короля, що містив 500 символів.

Нічого не рухає технології так швидко як війна і бажання отримати перевагу над ворогом. Але період першої світової війни не мав революційних подій в сфері криптографії, в цей вдосконалювали існуюче. Наприклад німці використовували шифр ADFGVX, предком якого був ADFGX.

А от період другої світової війни можна назвати революцією завдяки використанню машини Еніґма та бомби Тьюрінга. Саме за їх прикладом пішли майбутні методи шифрування. Та саме на цих ідеях базується розробка квантового комп'ютера.

На сучасному етапі в процесі шифрування та дешифрування використовують наступні математичні методи: арифметику остач, методи заміни та перестановки, метод шифрування за допомогою матриць, теорія множин, еліптичних кривих та ін.[2,3]. Так, наприклад, алгоритм симетричного шифрування AES працює методами підстановки і перестановки.

Таким чином, можна стверджувати, що застосування у процесах шифрування математичних методів є одним із ключових принципів їх реалізації.

Література

1. *https://sites.google.com/site/prokryptografia/who-we-are*
2. *https://essuir.sumdu.edu.ua/bitstream-download/123456789/20822/1/Filsh.pdf;jsessionid=04E314ADFB9478C7DDA415B8FBBC622A*
3. *https://bstudy.net/708022/informatika/osnovy_asimmetrichnogo_shifrovaniya*

УДК 368.016

І.В. Рассоха, к.ф.-м. н.,доцент
А.Б. Фесенко, студент групи 102ТН,
К.Ю. Шупик, студентка групи 102ТН,
А.В. Курнаков, студент групи 103ТН,
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ЗАСТОСУВАННЯ ТЕОРІЇ ПОДІЛЬНОСТІ У КРИПТОГРАФІЇ

Системи шифрування, що застосовуються в криптографічних системах мережі Інтернет (RSA, ElGamal, Shamir та ін) використовують останні досягнення теорії чисел та алгебри. Зламати їх — значить розв'язати складні математичні завдання. Основне завдання, яке переслідує