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

математика в криптографії — це криптографічна стійкість, тобто здатність протистояти теоретичному і практичному злому.

Методи та результати різних розділів математики використовуються як при розробці шифрів, так і при їх дослідженнях, зокрема, під час пошуку методів їх розкриття. Наприклад, у криптографії та криптоаналізі часто буває необхідно скласти дві послідовності чисел або відняти одну з іншої. Таке додавання і віднімання проводиться, зазвичай, не з допомогою звичайних арифметичних дій, а за допомогою операцій, званих модульною арифметикою.

Яскравим прикладом застосування подільності чисел є криптографічний алгоритм з відкритим ключем **RSA** (абревіатура від прізвищ Rivest, Shamir та Adleman), що базується на обчислювальній складності задач розкладання великих цілих чисел на прості множники [1]. Схема RSA отримала найширше визнання та реалізована практично у всіх додатках шифрування з відкритим ключем. RSA є блоковим шифром, в якому відкритий і шифрований текст представляється цілими числами з діапазону від 0 до n-1 для деякого n.

Алгоритм RSA складається з 4 етапів: генерації ключів, шифрування, розшифрування та розповсюдження ключів [2].

Щоб зашифрувати та розшифрувати яку-небудь інформацію, необхідна пара ключів – відкритий та закритий. Для їх виготовлення знадобиться пара простих чисел p і q. Наступний етап у виготовленні ключів - одержання числа n, що дорівнює добутку цих чисел. Тепер потрібно обчислити величину Ф (n), тобто функцію Ейлера, яка називається мірою стійкості числа до зламування, за формулою:

$$Ф = (p - 1)\times(q - 1)$$

Наступний крок - підбір числа e, яке має відповідати двом критеріям:

бути менше n і не мати спільних множників з Ф (n).

І останнє – треба знайти число d таке, що:

$$d \times e \bmod Ф(n) = 1,$$

де M – число, що шифрується.

Тепер ми маємо пари чисел:

(n, e) – відкритий ключ;

(d, n) – закритий ключ.

Для розшифровування числа скористаємося формулою:

$$Cd(\bmod n) = M$$

Таким чином, ми розшифрували наше число M.

Безпека RSA заснована на тому факті, що маючи велике число n (що є добутком двох простих чисел p і q), розкласти його на прості множники, не знаючи цих чисел зробити важко. Розробники несуть відповідальність за вибір простих чисел, що становлять модуль RSA

Надійність RSA багато в чому забезпечується тим, що при використанні досить довгих чисел, розкласти їх добуток на складові множники за

прийнятний час поки що не вдається, хоча існує ряд атак, що використовують специфічні прорахунки при шифруванні. Очікується, що зі створенням квантових комп'ютерів від алгоритму RSA доведеться відмовитися, оскільки вони можуть швидко розкладати на множники довгі цілі числа [3].

В даний час криптографічна система RSA отримала широке поширення. Вона була першою системою, здатною і для шифрування, і для цифрового підпису. Зараз вона використовується в великому числі криптографічних додатків, також її використовують в поєднанні з симетричними криптосистемами. Наука не стоїть на місці. Обчислювальні машини стають ще потужнішими, з їх допомогою можна вирішити все більш і більш складні задачі. Тому і криптографія повинна постійно удосконалювати свої методи, для того, щоб зуміти протидіяти шахраям. Часто це вдається зробити, залучаючи математичні методи.

Література

1. https://uk.wikipedia.org/wiki/Подільність
2. https://uk.wikipedia.org/wiki/RSA
3. https://studwood.net/1685074/informatika/preimuschestva_nedostatki_algoritma_shifrovaniya

УДК 368.016

І.В. Рассоха, к.ф.-м.н., доцент,
Т.О. Ширмовська, студентка гр. 101-ФМ,
М.Ю. Бєлодєд, студент гр. 101-ФМ
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ВИКОРИСТАННЯ СКЛАДНИХ ВІДСОТКІВ ДЛЯ РОЗРАХУНКУ ВАРТОСТІ ОБЛІГАЦІЙ КОРПОРАЦІЙ ПРОВІДНИХ КРАЇН СВІТУ

Математичне моделювання економічних процесів є потужнім інструментом не тільки вивчення сучасних тенденція світової економіки, а й може з успіхом бути використане для мотивації вивчення математики студентами відповідних спеціальностей. Тому наведемо приклад однієї з таких задач, в якій розглядається поняття складних відсотків.

Облігація (eng: bond) — вид цінних паперів, що має певну вартість, встановлювану емітентом (організацією продавця) і гарантує, що вартість буде виплачена покупцеві у вигляді грошей або майна протягом визначеного продавцем часу [1]. Складні відсотки – відсотки, які нараховуються на початкову суму інвестицій та на відсотки, нараховані з попередніх періодів. Для застосування складених процентних ставок достатньо реінвестувати дохід [2].