УДК 514.18

О.С. ЛЕБІДЬКО, А.В. НАЙДИШ, В.В. КУЧЕРЕНКО
Мелітопольська школа прикладної геометрії
Мелітопольський державний педагогічний університет імені Богдана Хмельницького

ВЗАЄМОЗВ'ЯЗОК ГЕОМЕТРИЧНИХ ОБ'ЄКТІВ ТА КРИПТОГРАФІЇ

Проводиться аналіз взаємозв'язку різноманітних геометричних об'єктів та історичного розвитку криптографії.

Ключові слова: криптографія, шифрування, геометричні об'єкти, еліптична крива.

О.С. ЛЕБЕДЬКО, А.В. НАЙДЫШ, В.В. КУЧЕРЕНКО
Мелитопольская школа прикладной геометрии
Мелитопольский государственный педагогический университет имени Богдана Хмельницкого

ВЗАИМОСВЯЗЬ ГЕОМЕТРИЧЕСКИХ ОБЪЕКТОВ И КРИПТОГРАФИИ

Проводится анализ взаимосвязи разнообразных геометрических объектов и исторического развития криптографии.

Ключевые слова: криптография, шифрования, геометрические объекты, эллиптическая кривая.

O.LEBIDKO, A.NAJDISH, *V.KUCHERENKO*
Melitopol School of Applied Geometry
Melitopol State Pedagogical University named Bohdan Khmelnytsky

INTERRELATION OF GEOMETRIC OBJECTS AND CRYPTOGRAPHY

The analysis of interrelation of various geometric objects and historical development of cryptography.

Keywords: cryptography, encryption, geometric objects, elliptic curve.

Постановка проблеми

Одною з актуальних проблем, є активне застосування у кіберзлочинності обчислювальних можливостей сучасних ЕОМ, стрімко зростають. Так, на щорічній міжнародній конференції Black Hat (Лас-Вегас, 2013 р.) з особливим зверненням виступила група фахівців з кібербезпеки. У зверненні було наголошено: існуючі алгоритми, на яких базується сучасна криптографія, знаходяться у небезпеці через швидкий розвиток автоматизованого розв'язання математичних задач, тому необхідно розробляти нові методи криптографії [1]. Тобто, була сформульована загальна науково-прикладна проблема криптографії: розробка нових алгоритмів для шифрування та захисту даних на принципово нових засадах.

Аналіз останніх досліджень

Відомі [2, 6] підходи та методи криптографії (шифрування) мають суто геометричний зміст або ж геометричну інтерпретацію (модель). Причому, розглядаючи еволюцію криптографії як науково-прикладної галузі, можна дійти висновку, що розвиток ідей та методів криптографії дуже тісно пов'язаний (зумовлений) з ходом еволюції математики: від натуральних чисел, наочних геометричних фігур та побудов до сучасного абстрактно-понятійного апарату. Виходячи з цього факту та розглядаючи еволюцію криптографічних методів приходимо до висновку, що одним з напрямів розв'язання вище сформульованої проблеми криптографії є залучення нових геометричних ідей та методів геометричного моделювання.

Первинні міркування щодо напряму пошуку розв'язання проблеми та його концептуальні засади, що витікають з аналізу сучасного стану проблеми, були сформульовані у роботі [2], але ще одним важливим міркуванням при цьому є дослідження еволюції ідей та методів криптографії.

Формування цілей статті

Провести аналіз історичного розвитку та взаємозв'язку геометричних об'єктів у задачах криптографії з метою виявлення та уточнення основних напрямів та умов пошуку шляхів розвитку методів криптографії на засадах апарату геометричного моделювання.

Основна частина

Для подальшого аналізу необхідно чітко визначити деякі поняття та терміни криптографії.

Криптографія (від грецького kryptós – прихований і gráphein – писати) – наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації стороннім) і автентичності (цілісності і справжності авторства) інформації [2].

Шифрування — оборотне перетворення даних, з метою приховання інформації, за допомогою математичних або геометричних способів [3].

Серед різновидів шифрування можна виділити 2 групи: шифри перестановки та шифри заміни (підстановки).

Шифр простої заміни – клас методів шифрування, які зводяться до створення за певним алгоритмом таблиці шифрування, в якій для кожної літери відкритого тексту існує єдина відповідна їй літера шифр-тексту [4].

Шифр підстановки – це метод шифрування, у якому елементи вихідного відкритого тексту замінюються зашифрованим текстом у відповідності до деяких правил [5].

Розглянемо взаємозв'язок способів шифрування та геометричних об'єктів, задіяних при цьому (табл. 1).

Таблиця 1.

Взаємозв'язок способів шифрування і геометричних об'єктів

Геометрична фігура	Назва шифру
Циліндр (конус)	Шифр Сцитала
Відрізок	Шифр Цезаря лінійка Енея
Коло	Диск Альберті
Квадрат	"Магічний квадрат" Квадрат Полібія
Прямокутник	Шифр перестановки за групам Шифр Чейза
Трикутник	Шифр Уілкінса
Крива	Шифр на базі еліптичних кривих

Одним з найперших шифрувальних засобів був жезл "Сцитала" (циліндр), який використовувався у V віці до н.е. Шифр "Сцитала" має наступний вигляд: *m* – кількість витків на циліндрі, *n* – кількість літер, розташованих на одному витку. Отже ключом шифру є числа *m* та *nm*, що визначаються діаметр циліндра та довжину стрічки.

Із терміном "відрізок" пов'язано декілька технік шифрування, в основу яких покладена відстань (відрізок) між знаходженням символів у відкритому та закритому повідомленнях.

Принцип дії шифру Цезаря і лінійки Енея полягає в тому, щоб послідовно зсунути алфавіт на певну відстань, а ключ – це відстань (відрізок) між літерами, на які робиться зсув (рис. 1).

Рис. 1. Шифр із застосування відрізків

Прикладом шифрування із застосування кола є шифр Альберті, який представляє собою механічний шифрувальний диск, що працював наступним чином: у середині великого зовнішнього диску знаходився рухомий внутрішній диск, обидва з круговими алфавітами. Щоб прочитати шифр, адресат повинен був знати взаємне положення дисків.

Шифри із використанням квадратів ("магічні квадрати", "квадрат Полібія") базуються на такому принципі: літери алфавіту записуються у квадрат, таким чином, зашифроване повідомлення буде мати вигляд послідовного набору чисел, що відповідають номеру рядку і стовбця для кожної літера, наприклад, А → 1.1, Б → 1.2, В → 1.3 і т.д.

Прикладом шифрування на основі трикутників є шифр Уілкінсона (рис. 2), у якому криптограма мала вигляд невинних геометричних фігур. Передавалось лише зображення. Ключем шифру є верхня послідовність літер і відстаней між ними. Такий змішаний підхід до захисту інформації активно використовується і в теперішній час.

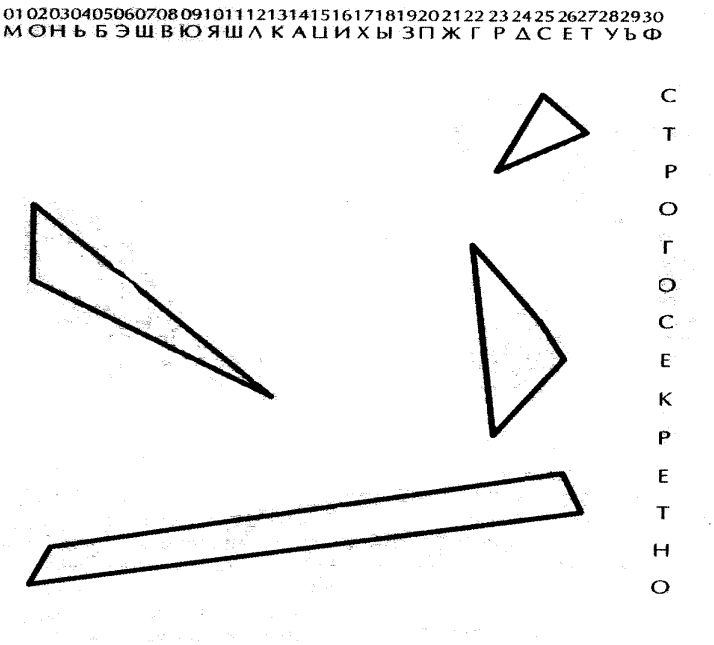

Рис. 2. Шифр Уілкінса

На теперішній час активного розвитку набуває шифрування із використанням різноманітних кривих, найбільш розповсюдженим є шифрування на базі еліптичних кривих [1]. Особливістю еліптичних кривих є те, що пряма перетинає таку криву максимум у трьох точках, а якщо пряма – дотична, то точка дотику враховується за дві однакові точки (рис. 3). У криптографії еліптичні криві утворюють самостійний розділ еліптичної криптографії, який присвячено вивченню криптосистем на базі еліптичних кривих, зокрема на еліптичних кривих базується російський стандарт ГОСТ Р 34.10-2001, що описує алгоритми формування та перевірки електронного цифрового підпису.

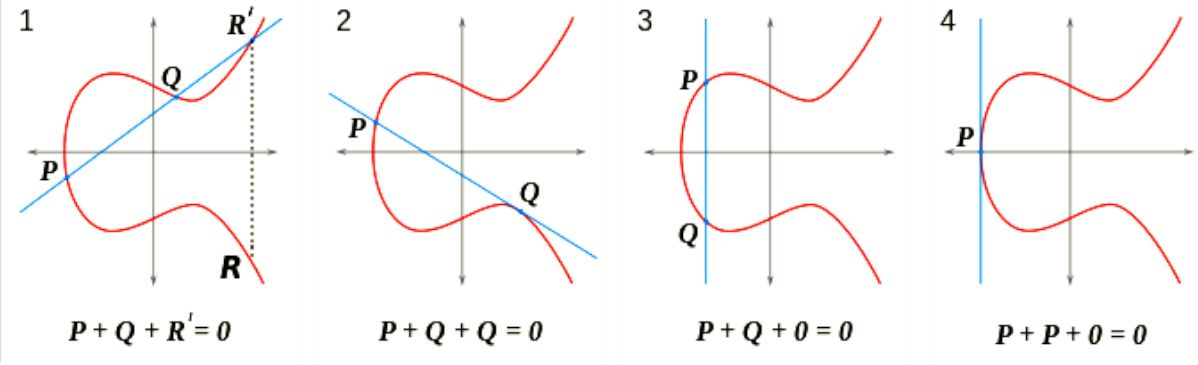

Рис. 3. Приклад еліптичної кривої

Проаналізувавши історичний розвиток взаємозв'язку криптографії та геометричних об'єктів можна зробити висновок, що задачі шифрування та дешифрування зводяться до позиційних та метричних задач прикладної геометрії, зокрема розвиток способів шифрування базується на збільшенні складності виду та ступеню геометричного образу аналогу.

Опираючись на [2] можна зробити припущення, що подальший розвиток криптографії буде базуватися не на ускладненні апарату еліптичних кривих, а на розвитку із залученням принципово нового математичного апарату. Сформулюємо вимоги, яким повинен відповідати новий сучасний метод криптографії:

- мінімізація похибки;
- можливість моделювання кривих із наперед заданими властивостями;
- варіативність модельованих кривих;
- спільність підходу для різних видів кривих;
- простота програмної реалізації.

Опираючись на ці вимоги, доречним, на наш погляд, буде використання апарату БН-числення, серед особливостей якого можна відмітити наступне:

- БН-числення дозволяє використовувати функціонали для визначення геометричних об’єктів;
- точкові рівняння геометричних образів інваріантні відносно мірності простору глобальної системи координат;
- дискретні вихідні дані – дискретний результат;
- кожній геометричній операції ставиться у відповідність аналітична операція;
- простота подальшої програмної реалізації алгоритмів і способів.

Виходячи із вище наведеного доречно буде звернути увагу на можливість вирішення задач криптографії способами апарату БН-числення.

Висновки

Було проведено аналіз історичного розвитку способів шифрування та взаємовідповідність елементарним геометричним об’єктам – складність та специфіка задачі визначає складність та геометричний сенс способу шифрування. Розглядаючи історичну ретроспективу еволюції способів шифрування можна зробити наступні висновки:

- збільшення виду і складності базової кривої геометричного об’єкту;
- застосування якісно нових замість застарілих підходів зсуву та заміни;
- розвиток принципово нових математичних апаратів для застосування у криптографії.

Також необхідно відмітити, що якщо відкинути формальні вимоги задачі шифрування, то, виходячи з табл. 1, отримуємо значну область варіацій для задач шифрування, а завдяки комбінації різноманітних геометричних об’єктів та їх властивостей можна значно збільшити складність шифру.

На наш погляд, у подальших дослідженнях з даної тематики доречно розвивати математичних апарат геометричного моделювання БН-числення як перспективного та принципово нового апарату для розв’язку задач криптографії.

Список використаної літератури

1. Эксперты призывают готовиться к криптоапокалипсису [Електронний ресурс].– Режим доступу: URL: http://habrahabr.ru/post/188846/.
2. Лебідько О.С. Місце еліптичних кривих у криптографії та можливості удосконалення їх геометричного апарату / О.С. Лебідько, А.О. Бездітний, А.В. Найдиш, В.В. Кучеренко // Прикладна геометрія та інженерна графіка: міжвід. наук.-техн. збірник / КНУБА.– К., 2014.– Вип. 92
3. Frederick C.Mish Merriam-Webster's Collegiate Dictionary, Eleventh Edition.– Merriam-Webster, 2003
4. Menezes Alfred J. Handbook of applied cryptography / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone.– CRC-Press, 1996.– С. 32.
5. Шнайер Б. Подстановочные шифры / Б. Шнайер // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с.
6. Саймон Сингх Книга шифров. Тайная история шифров и их расшифровки.– АСТ, 2007 – 446 с.