УДК 004.056.55+51

А. А. Коломієць
А. С. Сухоребра

МАТЕМАТИКА ТА КРИПТОГРАФІЯ

Вінницький національний технічний університет

Анотація. *У статті розкрито аспекти розвитку та функціонування криптографії, наведено приклади застосування математичного апарату.*
Ключові слова: *криптографія, математика, шифри*

Abstract *The aspects of development and functioning of cryptography are exposed in the article the examples of the use of mathematical apparatus are given.*
Key words*: cryptography, mathematics, ciphers*

Важливою областю застосування математики є криптографія − наука про шифри: способи перетворення інформації, що дозволяють приховувати її зміст від сторонніх. Основна функція криптографії − надання конфіденційності. Найважливіший рівень захисту інформації − криптографічний, він являє собою шифрування даних з метою приховати їхній зміст. Доти, поки користувач не ідентифікований по ключу, зміст даних йому недоступний. Дані в цьому випадку розглядаються як повідомлення, і для захисту їхнього змісту використовується класична техніка шифрування. Криптографія припускає наявність трьох компонентів: даних, ключа й криптографічного перетворення. [4, С.10].

Перші спроби шифрування були ще за чотири століття до нашої ери.

До наших днів дійшов шифр Цезаря: потрібно читати щораз четверту букву замість першої, наприклад, *D* замість *A* і так далі. Послання сенату VENI VIDI VICI, тобто ПРИЙШОВ ПОБАЧИВ ПЕРЕМІГ, зроблене Цезарем виглядало б шифровкою SBKF SFAF SFZF.

До XVIII століття криптографія остаточно сформувалася як наука.

Шифр Хілла

Починаємо з вибору m − буквеного алфавіту й кодуємо кожну букву одним числом із множини $\{0,1,2,...,m-1\}$. Нехай алфавіт містить 33 літери алфавіту української мови (тобто $m = 33$):

А	Б		В	…	Ю	Я
0	1		2	…	31	32

Тепер будемо ставити у відповідність кожній біграмі (α, β) таке число

$$P = 33\alpha + \beta \in \{0,1,..., 33^2 - 1\}.$$

Наприклад, біграмі «НІ» є відповідним ціле натуральне число $P = 33 \cdot 17 + 11 = 572$. Далі, зручно мати прості правила або функції шифрування й розшифрування. Ці функції повинні здійснювати ін'єктивне відображення:

$$P \xrightarrow{f} C \xrightarrow{f^{-1}} P,$$

де P − множина відкритих повідомлень (у цьому випадку біграм), але вже у формі чисел із множини $Z / 33^2 Z = \{0,1,..., 33^2 - 1\}.$

Функція шифрування повинна здійснювати перестановку на множині $Z/33^2Z$. Вибір відображення f, що шифрує, найпростіше взяти у вигляді афінного перетворення:

$$C = aP + b \ (\mathrm{mod}\ N^2).$$

Тут a , b − цілі числа, $N = 33$.

Для того, щоб існувало обернене відображення необхідно вимагати, щоб $(a, N^2) = 1$. Тобто, a і N^2 прості. У цьому випадку:

$$P = f^{-1}(C) = a^{-1}C - a^{-1}b \ (\mathrm{mod}\ N^2).$$

Для текстових файлів частіше інших уживається кодування Хаффмана, яке полягає в тому, що символи тексту заміняються послідовностями біт різної довжини. Чим частіше символ, тим коротша відповідна послідовність.

Розглянемо класичну схему передачі секретних повідомлень криптографічним перетворенням, де зазначені етапи й учасники цього процесу.

	Шифрування	Передача	Розшифрування
ТЕКСТ	листок	→	листок
КЛЮЧ	конверт	→	конверт
	Відправник	Канал зв'язку	Одержувач

Відправником шифрується повідомлення за допомогою ключа, і отримане шифрування передається по звичайному відкритому каналу зв'язку одержувачеві, у той час як ключ відправляється йому по закритому каналу, що гарантує таємність [4].

Методи і результати різних розділів математики (зокрема, алгебри, комбінаторики, теорії чисел, теорії алгоритмів, теорії ймовірностей і математичної статистики) використовуються як при розробці шифрів, так і при їх дослідженнях, зокрема, при пошуку методів розкриття шифрів. Шифр можна вважати стійким, поки при його дослідженні не виявляються особливості, які потенційно можна використовувати для розкриття шифру. Для користувачів шифру дуже важливо дізнатися, що він ненадійний, раніше, ніж цим зможуть скористатися зловмисники. Великий вплив на розвиток криптографії зробили роботи американського математика Клода Шеннона (1948 р.). Саме *Клод Шеннон* вперше почав вивчати *криптографію*, використовуючи системний підхід. Шеннон (якого вважають "батьком" теорії інформації) першим почав розглядати повідомлення і шуми в канал зв'язку з точки зору статистики, розглядаючи як кінцеві множини повідомлень, так і неперервні множини повідомлень [6].

Перша теорема Шеннона

Нехай джерело повідомлень має ентропію H (біт на символ), а C − пропускна здатність каналу (біт в секунду). Тоді можливо таке кодування інформації, при якому середня швидкість передачі через даний канал буде дорівнювати C / H= ε символів в секунду, де ε − як завгодно мала величина. Середня швидкість передачі даних не може бути більше C / H

Друга теорема *Шеннона*

Нехай джерело повідомлень має ентропію H на одну секунду, а C − пропускна здатність каналу. Якщо H ≤ C, то можливо таке кодування інформації, при якому дані джерела будуть передані через канал із як завгодно малою кількістю помилок. Якщо H > C, то можливо кодування, при якому неоднозначність отриманої інформації буде менше, ніж
H − C = ε, де ε − як завгодно мала величина. Додатково, не існує методів кодування, які дадуть неоднозначність менше ніж H-C.

Наслідок з другої теореми Шеннона

Нехай R − швидкість передачі інформації джерелом повідомлень, а C − пропускна здатність каналу. Тоді R < C, і можливо таке кодування інформації, при якому кількість помилкових біт в одиницю часу буде менше будь-який заздалегідь обраної позитивної константи ε.

Теорія Шеннона була точно сформульованою математичною задачею і дала можливість інженерам визначати ємність комунікаційного каналу.

Є 3 підходи для визначення кількості інформації:

Ентропійний підхід

Кількість інформації в повідомленні визначається тим, наскільки зменшиться невизначеність після одержання повідомлення. З цього погляду, кількість інформації, що міститься в отриманому повідомленні, є тим більшою, чим більшою була невизначеність до передачі повідомлення.

В основі теорії інформації лежить запропонований Шенноном спосіб обчислення кількості інформації як випадкової величини відносно іншої випадкової величини. Для дискретних випадкових величин X і Y, заданих законами розподілу $P(\mathrm{X}=\mathrm{X}_i)=\mathrm{p}_i$ $P(\mathrm{Y}=\mathrm{Y}_j)=\mathrm{p}_j$ і спільним законом розподілу $P(\mathrm{X}=\mathrm{X}_i,\mathrm{Y}=\mathrm{Y}_j)=\mathrm{p}_{ij}$ кількість інформації в X відносно Y, дорівнює

$$I(\mathrm{X},\mathrm{Y})=\sum_{i,j} p_{i,j}\log_2\frac{p_{i,j}}{p_i q_j}$$

Об'ємний підхід

Під обсягом інформації в повідомленні мають на увазі кількість символів цього повідомлення. Обсяг інформації – це досить груба кількісна характеристика інформації, оскільки суттєво залежить від форми подання інформації.

Алгоритмічний підхід

Згідно з алгоритмічним підходом за кількість інформації приймається значення деякої функції від складності кожного з об'єктів і довжини програми (алгоритму) перетворення одного об'єкта в інший. Інтуїтивно зрозуміло, що комп'ютерна програма, яка друкує повідомлення, що містить тільки нулі, украй проста. Усе, що потрібно робити цій програмі, – це друкувати один і той самий символ – нуль. Якщо ж повідомлення являє собою деяку послідовність, яка не підпорядковується ніяким закономірностям, то таке повідомлення не може бути реалізоване жодною "простою" програмою. У цьому випадку, довжина програми буде близька до довжини самої послідовності. Таким чином, кількість інформації в повідомленні визначається складністю програми, яка здатна відтворити це повідомлення – послідовність символів.

$I=L[\mathrm{G}(\mathrm{A},\mathrm{B})]$, де A – вхідний об'єкт, B – вихідний об'єкт, G – перетворююча програма, I – функція, за допомогою якої ми отримуємо розмір програми в байтах чи бітах.

Математичними основами криптографії є: відношення еквівалентності, відображення, групи, підгрупи, циклічні групи, симетрична група, кільце, підкільця, ідеали, фактор-кільця, кільце многочленів з коефіцієнтами з поля, алгоритм ділення Евкліда, поля, скінчення поля, класи лишків, визначення, цілі числа за модулем n, символи Лежандра і Якобі та числа Бюмана.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Анохін М. А., Варновский Н. П., Сидельников В. М., Ященко В. В. Криптографія в банківській справі, МИФИ, 1997.2. Дориченко С. А., Ященко В. В. 25 етюдів про шифри. – М.: "Теис", 1994.
2. Жельніков В. Криптографія від папіруса до комп'ютера – ABF, 1996. – 335 с.
3. Коробейников А. Г. Математичні основи криптографії. Навчальний посібник. С. Пб: ГИТМО (ТУ), 2002. - 41 с.
4. Математичні основи криптографії: конспект лекцій / В. А. Фільштінський, А. В. Бережний. – Суми: Сумський державний університет, 2011. – 138 с.
5. https://coin-lab.ru/stati-page/kriptovalyuta-i-kriptografiya-istoriya-vozniknoveniya/
6. http://book.etudes.ru/toc/cryptography/

Науковий керівник ***Альона Анатоліївна Коломієць*** — к. пед. наук, доцент кафедри вищої математики, Вінницький національний технічний університет, Вінниця, e-mail: alona.kolomiets.vnt@gmail.com

Alona A. Kolomiets — Cand. Sc. (Eng), Assistant Professor of Vinnytsia National Technical University, Vinnytsia

Ангеліна Сергіївна Сухоребра — студентка 1 курсу ФІТКІ, групи 2БС-17б, Вінницький національний технічний університет, Вінниця, e-mail: suhorebraabgelina@gmail.com

Angelina Sergiivna Suhorebra - *student of Department of Informatic Technologies and Computer Engineering, Vinnitsa National Technical University, Vinnytsia, e-mail: suhorebraabgelina@gmail.com.*