DOI: 10.58168/OpEq2025_146-153
УДК 003.26

# ЧИСЛА БЕРНУЛЛИ В КРИПТОГРАФИИ

BERNULLI NUMBERS IN CRYPTOGRAPHY

**Полтарабатько Роман Сергеевич**
студент 4 курса факультета прикладной математики, информатики и механики ВГУ, г. Воронеж, Россия
**Poltarabatko Roman Sergeevich**
4th year student of the Faculty of Applied Mathematics, Computer Science and Mechanics of VSU, Voronezh, Russia

**Аннотация.** В данной статье рассматривается метод шифрования, основанный на числах Бернулли. Приводится математическое описание метода, включая рекуррентные соотношения для генерации чисел Бернулли, а также алгоритм их применения в криптографическом шифре. Реализован алгоритм преобразования текста в числовую последовательность с последующим шифрованием и расшифрованием на основе арифметических операций с числами Бернулли.

**Abstract.** This paper presents an encryption method based on Bernoulli numbers. A mathematical description of the method is given, including recurrence relations for generating Bernoulli numbers and an algorithm for their application in a cryptographic cipher. The algorithm for converting text into a numerical sequence is implemented, followed by encryption and decryption based on arithmetic operations with Bernoulli numbers.

**Ключевые слова:** шифрование, числа Бернулли, криптография, безопасность данных, рекуррентные соотношения.

**Keywords**: encryption, Bernoulli numbers, cryptography, data security, recurrence relations.

Числа Бернулли — это последовательность рациональных чисел, возникающих в ряде Тейлора функции $\frac{x}{e^x-1}$. Они обозначаются как $B_n$ и используются, например, при вычислении значений сумм степеней натуральных чисел, в разложениях и аналитических выражениях.

Числа Бернулли определяются рекуррентным соотношением

$$B_0 = 1, \quad B_n = -\frac{1}{n+1}\sum_{k=1}^{n}\binom{n+1}{k+1}B_{n-k}\ , \qquad n \in N.$$

Первые числа Бернулли:

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}, \ldots.$$

Отметим, что нечётные индексы (кроме первого) дают нулевые значения.

Числа Бернулли представляют собой важную и широко изучаемую последовательность в математике, которая обладает уникальными свойствами и играет значительную роль в различных областях науки, таких как теория чисел, анализ, комбинаторика и криптография.

Одной из ключевых особенностей чисел Бернулли является их подчинение строго определённым рекуррентным соотношениям. Эти соотношения обеспечивают возможность последовательного вычисления чисел Бернулли, опираясь на значения, которые были найдены на предыдущих этапах. Такой подход делает процесс их вычисления систематизированным и предсказуемым, что особенно важно при их применении в задачах с высокой степенью вычислительной сложности.

Основное рекуррентное соотношение для чисел Бернулли [1] имеет следующий вид:

$$\sum_{k=0}^{n} \binom{m+1}{k} B_k = 0 \quad (1)$$

где $\binom{m+1}{k} = \frac{(m+1)!}{k!(m+1-k)!}$ — биномиальный коэффициент, описывающий количество способов выбрать $k$ элементов из $m+1$ элементов. Свойства этого соотношения:

1. $B_0 = 1$;

2. $B_1 = -\frac{1}{2}$;

3. $B_m = 0$ для всех нечетных $m > 1$.

Используя это рекуррентное соотношение, можно вычислить $B_m$ для любого $m$, зная значения для меньших индексов. Например, для $m = 2$:

$$\binom{3}{0} B_0 + \binom{3}{1} B_1 + \binom{3}{2} B_2 + \binom{3}{3} B_3 = 0$$

Подставляя известные значения $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_3 = 0$, можно найти $B_2$.

Числа Бернулли могут быть использованы для генерации матриц, применяемых в многослойных системах шифрования.

Матрица Бернулли $B_n$ [2] формируется на основе чисел Бернулли и используется для преобразования данных. Она имеет следующий вид (2):

$$B_n = \begin{pmatrix} B_{n-1} & B_n \\ B_n & B_{n+1} \end{pmatrix} \quad (2)$$

При n = 1 матрица $B_1$ имеет следующий вид (3):

$$B_1 = \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{6} \end{pmatrix} \quad (3)$$

Для n = 2 матрица расширяется, добавляя новые элементы (4):

$$B_2 = \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{6} & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (4)$$

Шифрование данных играет ключевую роль в обеспечении безопасности информации. Использование чисел Бернулли в криптографии позволяет создавать ключи со сложной структурой, что затрудняет их предсказание. Принцип шифрования заключается в преобразовании символов текста в числовые представления с последующим модифицированием с использованием чисел Бернулли [3].

Метод шифрования основан на поэтапном преобразовании исходного текста в числовую форму, его разбиении на блоки фиксированной длины и последовательном применении математических операций для получения зашифрованного сообщения. В процессе шифрования используется матричная трансформация, ключевым элементом которой является матрица $B_2$. Данная матрица строится с использованием чисел Бернулли и обладает особыми свойствами, обеспечивающими надежность преобразований. В зависимости от значений битов ключа шифрования матрица $B_2$ применяется в различных степенях к каждому блоку данных, что усложняет анализ зашифрованного текста и повышает криптографическую стойкость метода.

***Основные этапы алгоритма:***

**1. Отображение символов в числовой формат**

Каждому символу алфавита (включая пробелы и знаки препинания) сопоставляется уникальное число. Это позволяет представить текст в виде числового вектора.

**2. Формирование матрицы данных**

Числовая последовательность разбивается на блоки фиксированной длины, которые формируют матрицу $q_0$, подлежащую шифрованию.

**3. Генерация ключа шифрования**

Ключ задается в виде бинарной последовательности (например, «10101»), где каждая цифра влияет на применяемые матричные преобразования. Для каждого бита ключа выбирается степень, в которую будет возводиться матрица $B_2$. Эта степень определяется по формуле (5):

$$exp = \left(\frac{i+1}{2}\right) + 1 \quad (5)$$

где i – индекс соответствующего бита.

**4. Матричные преобразования**

В зависимости от значения бита (например, «1» или «0») к исходной матрице данных $q_0$ применяется матричное преобразование с $B_2^{exp}$. Если бит равен «1», то происходит умножение текущего состояния данных на $B_2^{exp}$, что обозначается как обновление ветки branch1. Если бит равен «0», то применяется альтернативное ветвление (branch0), при этом часто используется результат, полученный ранее при обработке битов «1». Такой механизм изменения степени матричного преобразования в зависимости от ключа позволяет добиться дополнительного уровня нелинейности и защищенности шифра.

**5. Формирование зашифрованного сообщения**

Итоговая матрица содержит зашифрованные данные, которые впоследствии могут быть дешифрованы при наличии правильного ключа.

**6. Дешифрование**

Для восстановления исходного сообщения применяется обратный процесс. Зашифрованная матрица, полученная в результате последовательного применения степеней $B_2$, умножается на обратные матрицы $B_2^{-exp}$ в порядке, обратном порядку шифрования. Это позволяет отменить эффект каждого преобразования, восстановив исходное числовое представление данных.

Рассмотрим пример шифрования слова **«привет»**, ключ «**101**».

**1.** Пусть алфавит начинается с «а» = 0, «б» = 1, ..., «п» = 16, ..., «я» = 32. Тогда: «п» = 16, «р» = 17, «и» = 8, «в» = 2, «е» = 5, «т» = 19. Получаем числовой вектор $V = (16, 17, 9, 2, 5, 19)$.

**2.** Выберем размер блока $k = 3$, тогда вектор разбивается на два блока:

$$q_0 = \begin{pmatrix} 16 & 17 & 9 \\ 2 & 5 & 19 \end{pmatrix}$$

**3.** Ключ шифрования — трёхбитный. Для каждого бита по формуле $exp = \left(\frac{i+1}{2}\right) + 1$ определим степень: i = 0 → exp = 1, i = 1 → exp = 2, i = 2 → exp = 2.

**4.** Начинаем шифрование:

- **Шаг 1:** бит = 1, exp = 1

  $branch_1$ инициализируется: $branch_1 = q_0 * B_2^1$

$$branch_1 = \begin{pmatrix} 16 & 17 & 9 \\ 2 & 5 & 19 \end{pmatrix} * \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{6} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{15}{2} & -\frac{31}{6} & 9 \\ -\frac{1}{2} & -\frac{1}{6} & 19 \end{pmatrix}$$

- **Шаг 2:** бит = 0, exp = 2

  $branch_0$ инициализируется: $branch_0 = q_0 * B_2^2$

$$B_2^2 = \begin{pmatrix} \frac{5}{4} & -\frac{7}{12} & 0 \\ -\frac{7}{12} & \frac{5}{18} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$branch_0 = \begin{pmatrix} 16 & 17 & 9 \\ 2 & 5 & 19 \end{pmatrix} * \begin{pmatrix} \frac{5}{4} & -\frac{7}{12} & 0 \\ -\frac{7}{12} & \frac{5}{18} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{121}{12} & -\frac{83}{18} & 9 \\ -\frac{5}{12} & \frac{2}{9} & 19 \end{pmatrix}$$

- **Шаг 3:** бит = 1, exp = 2

  $branch_1$ обновляется: $branch_1 = branch_1 * B_2^2$

$$branch_1 = \begin{pmatrix} \frac{15}{2} & -\frac{31}{6} & 9 \\ -\frac{1}{2} & -\frac{1}{6} & 19 \end{pmatrix} * \begin{pmatrix} \frac{5}{4} & -\frac{7}{12} & 0 \\ -\frac{7}{12} & \frac{5}{18} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{223}{18} & -\frac{1255}{216} & 9 \\ -\frac{19}{36} & \frac{53}{216} & 19 \end{pmatrix}$$

Итоговое зашифрованное сообщение – это матрица $branch_1$.

**5.** Теперь расшифруем сообщение. Для этого найдем обратные матрицы для $B_2^2$ и $B_2^1$:

$$B_2^{-2} = \begin{pmatrix} 40 & 84 & 0 \\ 84 & 180 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B_2^{-1} = \begin{pmatrix} -2 & -6 & 0 \\ -6 & -12 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Далее, умножаем матрицу $branch_1$ сначала на $B_2^{-2}$:

$$\begin{pmatrix} \frac{223}{18} & -\frac{1255}{216} & 9 \\ -\frac{19}{36} & \frac{53}{216} & 19 \end{pmatrix} * \begin{pmatrix} 40 & 84 & 0 \\ 84 & 180 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{15}{2} & -\frac{31}{6} & 9 \\ -\frac{1}{2} & -\frac{1}{6} & 19 \end{pmatrix}$$

Затем полученную матрицу умножаем на $B_2^{-1}$:

$$\begin{pmatrix} \frac{15}{2} & -\frac{31}{6} & 9 \\ -\frac{1}{2} & -\frac{1}{6} & 19 \end{pmatrix} * \begin{pmatrix} -2 & -6 & 0 \\ -6 & -12 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 16 & 17 & 9 \\ 2 & 5 & 19 \end{pmatrix}$$

Это и есть исходная матрица $q_0$.

Использование чисел Бернулли в криптографии демонстрирует потенциал для создания алгоритмов, обладающих высокой степенью защиты благодаря сложности их структуры. Они могут быть использованы для генерации криптографических ключей, что затрудняет их анализ и взлом. В перспективе данный метод может быть усовершенствован и адаптирован для различных приложений в области защиты информации.

## Список литературы

1. Абрамовиц, М., Стиган, И. Справочник по математическим функциям с формулами, графиками и математическими таблицами. Издательство правительства США, 1972, стр. 824–825.

2. Мишра К. Л. П., Чандрашекхран Н., «Теория информатики» (3-е издание), PHI Learning, (2014).

3. Навалакхе, Р., Атре, Х. Криптографические алгоритмы с использованием конечного автомата, чисел Бернулли и чисел Люка. Журнал математики и математических наук Юго-Восточной Азии, Том 17, № 3, 2021, стр. 17-28.

## References

1. Abramowitz, M., Stegun, I.A. Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. US Government Printing Office, 1972, pp. 824–825.

2. Mishra K. L. P., Chandrashekhran N., Theory of Computer Science, (3rd Edition) PHI Learning, (2014).

3. Navalakhe, R., Atre, H. Cryptographic Algorithms Using Finite State Machine, Bernoulli and Lucas Numbers. South East Asian J. of Mathematics and Mathematical Sciences, Vol. 17, No. 3, 2021, pp. 17-28.