УДК 003.26:511.176

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ: ПРИМЕНЕНИЕ ПОСЛЕДОВАТЕЛЬНОСТИ ФИБОНАЧЧИ

Болбас К.В., Филипова А.Д., студенты

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лущакова И.Н. – канд. физ.-мат. наук, доцент

Аннотация. В статье исследована возможность применения последовательности Фибоначчи для шифрования текстовых сообщений. Основная идея заключается в использовании индексов Фибоначчи как основы для перестановочного шифра. В статье приведены теоретические основы, описана собственная реализация алгоритма на Python, проведено тестирование на различных текстах и выполнен анализ криптостойкости. Полученные результаты показывают, что предложенный метод пригоден для учебных целей и может служить основой для более сложных систем шифрования, хотя в чистом виде не обеспечивает достаточной стойкости для серьёзных применений.

Ключевые слова: криптография, последовательность Фибоначчи, шифрование, период Пизано, алгоритм.

Проблема защиты информации возникает постоянно – начиная с паролей от социальных сетей и заканчивая банковскими данными. За последние годы мы все стали свидетелями нескольких громких утечек данных, что заставляет задуматься о надёжности современных методов шифрования. В данной работе предпринята попытка разобраться в математических основах криптографии на конкретном примере. Последовательность Фибоначчи привлекает внимание по нескольким причинам. Во-первых, она изучается ещё в школе, но при этом обладает глубокими свойствами. Во-вторых, существует множество попыток использовать эту последовательность в криптографии, что говорит о её потенциальной применимости [1, с. 45].

1.ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСЛЕДОВАТЕЛЬНОСТИ ФИБОНАЧЧИ

1.1. Математические свойства последовательности Фибоначчи. Последовательность Фибоначчи была описана европейским математиком Леонардо из Пизы (Фибоначчи) в трактате «Liber Abaci» в 1202 году при решении задачи о размножении кроликов [2, с. 456]. Рекуррентное соотношение записывается следующим образом:

$$F_n = F_{n-1} + F_{n-2},$$ где $F_0 = 0$, $F_1 = 1$.

Здесь первые 20 чисел последовательности Фибоначчи следующие: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181.

Последовательность Фибоначчи обладает следующими свойствам:

- Тождество Кассини: $F(n-1) \cdot F(n+1) - F(n)^2 = (-1)^n$
- Период Пизано: если рассматривать последовательность по модулю m, она становится периодической. Обозначим период через $\pi(m)$. Например, для m = 10: f mod 10: 0, 1, 1, 2, 3, 5, 8, 3, 1, 4, 5, 9, 4, 3, 7, 0, 7, 7, 4, 1, 5, 6, 1, 7, 8, 5, 3, 8, 1, 9, 0, 9, 9, 8, 7, 5, 2, 7, 9, 6, 5, 1, 6, 7, 3, 0, 3, 3, 6, 9, 5, 4, 9, 3, 2, 5, 7, 2, 9, 1, 0... Период повторяется через 60 чисел, таким образом $\pi(10) = 60$. Это свойство важно для нас, так как при шифровании работают с конечным алфавитом (например, 33 буквы русского языка или 256 символов ascii), и периодичность влияет на длину ключа.
- Представление Зекендорфа: любое натуральное число можно единственным образом представить как сумму не подряд идущих чисел Фибоначчи. Например:

17 = 13 + 3 + 1 = $F_7 + F_4 + F_2$,
20 = 13 + 5 + 2 = $F_7 + F_5 + F_3$.

Это свойство можно использовать для кодирования, но в нашей работе используется более простой подход.

1.2. Матричное представление. Возведение матрицы в степень позволяет быстро вычислять числа Фибоначчи:

$$\big[[1,1],[1,0]\big]^n = \big[[F(n+1), F(n)], [F(n), F(n-1)]\big]$$

Используя бинарное возведение в степень, можно найти $F(n)$ за o(log n) операций. Это использовалось в программной реализации для работы с длинными последовательностями.

2. РАЗРАБОТКА АЛГОРИТМА ШИФРОВАНИЯ

2.1. Описание алгоритма. Нами разработан перестановочный шифр на основе индексов Фибоначчи. Идея состоит в том, что символы исходного текста переставляются согласно позициям, задаваемым числами Фибоначчи.

Алгоритм 1 (шифрования):
Вход: текстовое сообщение
Выход: зашифрованный текст

1. Разбить сообщение на слова (разделители – пробелы и знаки препинания, сохраняем их отдельно).
2. Для каждого слова длины l сгенерировать последовательность Фибоначчи не превышающих l: 1, 1, 2, 3, 5, 8... (начинаем с 1, а не с 0, так как индексация символов с 1).
3. Выбрать символы слова с соответствующих позиций в порядке возрастания индексов.
4. Если индекс повторяется (что происходит с единицами), символ берётся соответствующее количество раз.
5. Сформировать зашифрованное слово из выбранных символов.

Пример ручного шифрования:
Слово: "криптография" (11 символов)
Индексы: 1 2 3 4 5 6 7 8 9 10 11
Буквы: к р и п т о г р а ф и я
Числа Фибоначчи ≤ 11: 1, 1, 2, 3, 5, 8
Выбираем:

- Позиция 1: к
- Позиция 1: к (повтор)
- Позиция 2: р
- Позиция 3: и
- Позиция 5: т
- Позиция 8: р

Зашифрованное слово: "ккритр". Как видно, результат сильно отличается от исходного, но сохраняется некоторая структура (повторяющиеся символы остаются повторяющимися).

2.2. Алгоритм однозначного дешифрования. Дешифрование выполняется получателем, который знает ключ (начальные значения a, b и сдвиг k) и длину исходного слова l.

Алгоритм 2 (однозначное дешифрование):

1. По длине слова l и ключу (a, b) восстановить последовательность чисел Фибоначчи, не превышающих l.
2. Применить тот же сдвиг k и вычислить использованные при шифровании индексы:

$$index = \{(i - 1 + k)\ mod\ L \mid i \in f_{ibs}\}$$

3. Определить, какие позиции зашифрованного слова соответствуют позициям исходного слова. Так как каждый индекс из массива $index$ однозначно указывает символ из какой позиции исходного слова был взят, получатель распределяет символы шифротекста опять по этим позициям.
4. Оставшиеся позиции (не вошедшие в индексы Фибоначчи) восстанавливаются из второй части шифротекста, которая передаётся вместе с основным зашифрованным словом.

Таким образом, дешифрование является однозначным при условии, что:

- Получатель знает ключ (a, b, k),
- Известна длина исходного слова l,
- Символы, не вошедшие в индексы Фибоначчи, переданы отдельно.

Дешифрование сложнее, так как нужно восстановить исходный порядок. Получатель должен знать:

- Длины исходных слов;
- Начальные значения последовательности (если используются обобщённые Фибоначчи).

Алгоритм 3 (дешифрование):

1. По длине слова восстановить использованные индексы Фибоначчи.
2. Распределить символы зашифрованного текста по этим позициям.
3. Оставшиеся позиции (не попавшие в последовательность Фибоначчи) заполнить, используя дополнительную информацию или оставив пустыми (в зависимости от варианта реализации).

В нашей реализации был использован вариант, где незадействованные символы просто отбрасываются (что делает шифр необратимым без дополнительного ключа), или сохраняются отдельно.

2.3. Улучшение алгоритма. Для повышения стойкости мы добавили несколько модификаций:

1. Модификация 1: обобщённые начальные значения. Вместо $F_1 = 1$, $F_2 = 2$ используем $F_1 = a$, $F_2 = b$, где a и b — часть ключа. Пример: a = 3, b = 7, последовательность: 3, 7, 10, 17, 27, 44...

2. Модификация 2: работа по модулю. Берём остатки по модулю длины слова: $F_n \ mod \ L$

3. Модификация 3: добавление сдвига. Каждый индекс сдвигается на константу k (вторая часть ключа): : $(F_n + k) \ mod \ L$

3. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ.

В данной работе реализован алгоритм на python. Основные функции: generate_fibonacci (генерация чисел Фибоначчи), fib_encrypt_word (шифрование одного слова), fib_encrypt_text (шифрование текста с сохранением разделителей).

4. АПРОБАЦИЯ И АНАЛИЗ РЕЗУЛЬТАТОВ

4.1. Тестирование на примерах. Проведём шифрование фразы из оригинальной работы для сравнения в таблице 1.

Таблица 1 – тестирование

Слово	Длина	Индексы Фибоначчи	Зашифровано
Математические	14	1,1,2,3,5,8,13	MMAAMTTE
Свойства	8	1,1,2,3,5,8	Ссвойств
Последовательности	18	1,1,2,3,5,8,13	Ппоопоследоват

4.2. Анализ частотного распределения. Была выполнена проверка, как шифрование влияет на частоту символов. Был использован текст романа "Война и мир" Л.Н. Толстого (фрагмент на 5000 символов).

Результаты:

- В открытом тексте: частота 'о' — 10.9%, 'е' — 8.2%, пробел — 17.3%
- В зашифрованном тексте: распределение более равномерное, но сохраняется корреляция с длиной слов

Проблема: в коротких словах (1-3 символа) шифрование практически не меняет текст, так как последовательность фибоначчи покрывает все позиции.

4.3. Оценка криптостойкости. Мы проанализировали устойчивость к основным атакам:

A) Атака полным перебором:

- Для базового варианта (стандартные Фибоначчи): пространство ключей = 1 (нет ключа) — шифр легко взламывается
- Для модификации с начальными значениями a, b ≤ 100: 10 000 вариантов — взламывается за секунды
- Для a, b ≤ 1000 + сдвиг 0-100: 100 000 000 вариантов — требуется несколько минут

B) Частотный анализ: шифр уязвим, так как сохраняет частоты символов внутри "Фибоначчиевых" позиций. Если злоумышленник знает алгоритм, он может восстановить часть текста.

C) Атака на основе известного открытого текста: если известна пара "открытый текст – шифротекст", ключ восстанавливается тривиально.

5. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Полученные результаты показывают, что разработанный алгоритм обладает как достоинствами, так и существенными недостатками

.

Достоинства:

- Простота реализации — базовый алгоритм укладывается в 20 строк кода
- Высокая скорость работы — шифрование текста на 1 мб занимает менее 0.1 секунды
- Не требует сложной математической подготовки для понимания

- При использовании обобщённых начальных значений даёт приемлемое для учебных целей пространство ключей

Недостатки:

- Критическая уязвимость: при отсутствии сдвига и обобщённых начальных значений алгоритм детерминирован — одинаковые слова шифруются одинаково
- Потеря информации: в базовом варианте часть символов (не попавших в индексы Фибоначчи) теряется
- Не подходит для коротких сообщений: в словах до 4 символов шифрование очевидно
- Требует передачи дополнительной информации для дешифрования (длины слов)

Возможные улучшения:

В ходе работы были придуманы несколько способов усилить алгоритм:

- Комбинировать с шифром цезаря (добавить сдвиг к каждому символу после перестановки)
- Использовать непоследовательные индексы Фибоначчи (например, только чётные или только простые индексы в последовательности)
- Применять разные начальные значения для каждого слова на основе общего ключа

Заключение. В ходе выполнения работы были изучены математические свойства последовательности Фибоначчи и предприняты попытки применить их для создания шифра. Разработанный алгоритм работает, но его криптостойкость оказалась недостаточной для практического применения без существенных модификаций. Основной вывод: чисто математические свойства (красота, периодичность, связь с золотым сечением) не гарантируют криптографической стойкости. Для надёжного шифра необходимо обеспечить диффузию и конфузию в терминах шеннона [7, с. 456] , что требует более сложных конструкций. Тем не менее, работа была полезна с учебной точки зрения: мы реализовали полный цикл криптографического исследования — от математической идеи до программной реализации и криптоанализа. Полученные навыки можно применить при изучении более серьёзных алгоритмов (aes, rsa).

Список использованных источников:

1. Кудояр, и.а. замечательные числа. Числа фибоначчи // первый шаг в науку. — 2015. — № 3. — с. 42-48.

2. Фибоначчи, л. Книга абака (liber abaci) / пер. С лат. — м.: наука, 1984. — 456 с.

3. Анисимов, с.ф., бигаева, л.а. применение метода фибоначчи для решения задач оптимизации // вестник бирского филиала уунит. — 2018. — т. 12. — с. 15-19.

4. Гончарова, к.е., матруненок, с.н. геометрические закономерности в природе // научные труды бгату. — минск, 2020. — с. 112-118.

5. Ишмухаметов, ш.т., мубараков, б.г. математические основы криптографии. Производящие функции: учебно-методическое пособие. — казань: казанский университет, 2021. — 156 с.

6. Панкратова, и.а. теоретико-числовые методы в криптографии: учебное пособие. — томск: тгу, 2009. — 204 с.

7. Шеннон, к. Теория связи в секретных системах // работы по теории информации и кибернетике. — м.: ил, 1963. — с. 243-332.

8. Столингс, в. Криптография и защита сетей: принципы и практика. — м.: вильямс, 2017. — 800 с. — с. 45-67 (глава 2: классические методы шифрования).

UDC 003.26:511.176

MATHEMATICAL FOUNDATIONS OF CRYPTOGRAPHY: APPLICATION OF THE FIBONACCI SEQUENCE

Bolbas K.V., Filipova A.D. students

Belarusian state university of informatics and radioelectronics, Minsk, republic of Belarus

Lushchakova i.n. – candidate of physical and mathematical sciences

Annotation. We investigate the possibility of using the Fibonacci sequence to encrypt text messages. The main idea is to use Fibonacci indices as the basis for a permutation cipher. The paper provides the theoretical foundations, describes our own implementation of the algorithm in Python, that was tested on various texts, and cryptographic strength analysis was performed. The results show that the proposed method is suitable for educational purposes and can serve as the basis for more complex encryption systems, although in its pure form it does not provide sufficient stability for serious applications.

Keywords: cryptography, Fibonacci sequence, encryption, Pisano period, algorithm.