# Информатика

**Душкин Роман Викторович**
*Директор по науке и технологиям Агентства Искусственного Интеллекта*

**Яхонтов Светозар Игоревич**
*Директор по развитию компаний StarForce и Safe'n'Sec, эксперт по информационной безопасности.*

## Книжный шифр

Мы продолжаем публиковать статьи из криптографического цикла Романа Душкина и Светозара Яхонтова. Настоящая статья посвящена одному из самых непростых для взлома шифров старых времён — книжному шифру. Фактически, если им пользоваться грамотно, то взломать криптограммы на его основе будет невозможно. А о том, как это сделать, вы узнаете далее в этой статье.

Сегодня мы рассмотрим довольно распространённый в старые времена метод шифрования секретных сообщений, который часто упоминается в художественной литературе и кинематографе — книжных шифр.

Историки сходятся во мнении, что создателем первых вариантов книжного шифра мог быть Эней Тактик (IV век до н. э.), древнегреческий военный и политический деятель, автор труда «О перенесении осады», в котором впервые упоминается описание книжного шифра. Упомянутый в труде книжный шифр был одним из способов передачи секретных сообщений между осаждёнными и их союзниками. Самой ценной для осаждённых информацией являются сведения о готовности союзников прийти на помощь и возможные сроки оказания военной помощи. Именно эта информация позволяет осаждённым принять решение о нормах распределения продовольствия и об условиях сдачи города, если военная помощь союзников не может быть оказана.

## Книжный шифр

Как не сложно догадаться, широкое распространение книжный шифр мог получить только с распространением промышленного книгопечатания, появлением паровых печатных машин, способных выпускать книги сравнительно большими тиражами — с середины XIX века. Применение книжного шифра предполагает наличие у участников тайной переписки одинакового издания — двух идентичных копий одной и той же книги. Буква в букву.

## Метод шифрования

Суть метода книжного шифра заключается в выборе информации из книги, где номера слов, начинающихся на определённую букву, или координаты самих букв выступают в качестве кодов символов исходного сообщения. В качестве координат часто используются номер страницы, номер строки и номер буквы в строке. При этом одной используемой букве может соответствовать несколько кодов (координат). Это делает книжный шифр не поддающимся атакам частотным методом — одной используемой в сообщении букве может соответствовать большое число вариантов координат, закономерность сопоставления которых можно определить только имея ключ — ту самую книгу, которую использовали для шифровки сообщения.

Использование книжного шифра было широко распространено в конце XIX — начале XX века в Российской Империи тайными революционными обществами. Этому способствовала потребность в методически простом в освоении методе шифрования, который при этом отличался высокой взломостойкостью. Ведь жандармские «чёрные кабинеты», ведущие перлюстрацию переписки известных им представителей таких обществ, были весьма продвинуты в части оснащённости и ресурсами, и методологией дешифровки тайных сообщений.

Однако у книжного шифра был и недостаток — логистический. Было необходимо хранить или, что сложнее, тайно перевозить с собой книгу, являющуюся ключом шифрования. Это вполне могло скомпрометировать тайную переписку в случае обнаружения некоторой идентичной книги в частом обороте у подозреваемых. Также сложно было вести переписку, находясь в заключении под арестом — доступ к книгам был весьма ограничен. В этом случае участники тайной переписки заучивали кодовые тексты книг наизусть.

В качестве примера кодового текста можно рассмотреть практику одной из переписок революционеров начала XX века — в качестве ключа используется стихотворение Н. А. Некрасова «Школьник». Стихотворение вписывалось в квадрат размером 10 на 10 букв (без пробелов и знаков препинания), если в строке было больше 10 букв, то лишние буквы выбрасывались:

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Н | У | П | О | Ш | Е | Л | Ж | Е | Р |
| 2 | Н | Е | Б | О | Е | Л | Ь | Н | И | К |
| 3 | Н | Е | В | Е | С | Е | Л | А | Я | Д |
| 4 | Э | Й | С | А | Д | И | С | Ь | К | О |
| 5 | Н | О | Г | И | Б | О | С | Ы | Г | Р |
| 6 | И | Е | Д | В | А | П | Р | И | К | Р |
| 7 | Н | Е | С | Т | Ы | Д | И | С | Я | Ч |
| 8 | Э | Т | О | М | Н | О | Г | И | Х | С |
| 9 | В | И | Ж | У | Я | В | К | О | Т | О |
| 10 | Т | А | К | У | Ч | И | Т | Ь | С | Я |

В качестве координат применяется дробь: числитель — номер строки, знаменатель — номер буквы в строке. Так слово «срочно» можно было зашифровать как: «4/3, 1/10, 2/4, 7/10, 8/5, 8/3» или «7/3, 5/10, 9/10, 10/5, 2/8, 5/6».

Однако столь простой ключевой текст применялся для возможности использовать его по памяти, без использования бумажного носителя ключевого текста. Стихотворение легко заучить наизусть, также легко оперировать координатами 10 на 10.

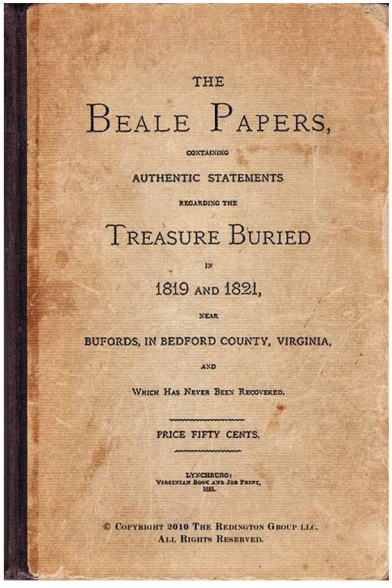
## Методы атаки

Действенным методом атаки в отношении книжного шифра является наблюдение за участниками переписки — какую книгу или текст они чаще всего используют в предполагаемый период времени обмена тайными сообщениями. Конечно, человек может перечитывать в течение своей жизни биографию Спинозы или «Комментарии к английским законам». Что всё-таки, наверное, может показаться подозрительным. Особенно, если самыми читаемыми являются конкретные страницы книги (что можно определить по засаленности таких страниц). А вот перевозить с собой целую библиотеку с книгами, используемыми для шифрования тайных сообщений, может быть не удобно. Внимание стоит уделить тем книгам, которые участник тайной переписки будет брать с собой в поездку.

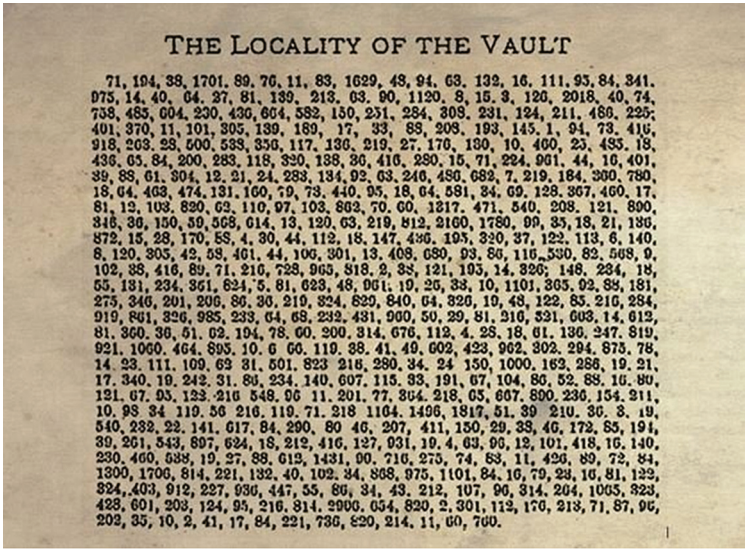
Примером стойкости этого метода шифрования являются «Шифрограммы Бейла» — три зашифрованных сообщения, датируемых 1822 годом, предположительно о местонахождении клада из золота, серебра и драгоценных камней, спрятанных на территории штата Вирджиния (США) экспедицией золотоискателей под предводительством Томаса Джефферсона Бейла. В первой шифрограмме, всё ещё не расшифрованной, как раз и содержится информация о местонахождении клада. Во второй шифрограмме, которую

смогли расшифровать в период 1845 – 1862 годов, содержится опись двух кладов, предположительная стоимость которых на сегодняшний день превышает 50 миллионов долларов США. Ключом к шифру оказался текст «Декларация независимости США» (поэтому никогда не стоит использовать широко доступные тексты). Третий шифр содержит перечень лиц из родственников участников экспедиции, которым человек, нашедший клад, должен передать две трети от найденного в случае, если никто из участников экспедиции не вернётся живым. Треть клада нашедший, как было указано в сопроводительном письме, может забрать себе.

Для привлечения ресурсов на расшифровку эти шифрограммы были опубликованы в 1865 году в книге неизвестного автора «Документы Бейла или книга, содержащая подлинные факты касательно сокровища, зарытого в 1819 и 1821 годах неподалеку от Бафордса, округ Бед-


THE
BEALE PAPERS,
CONTAINING
AUTHENTIC STATEMENTS
REGARDING THE
TREASURE BURIED
IN
1819 AND 1821,
NEAR
BUFORDS, IN BEDFORD COUNTY, VIRGINIA,
AND
WHICH HAS NEVER BEEN RECOVERED.
PRICE FIFTY CENTS.
LYNCHBURG:
VIRGINIAN BOOK AND JOB PRINT,
1885.


*Обложка книги «Документы Бейла или книга, содержащая подлинные факты касательно сокровища, зарытого в 1819 и 1821 годах неподалеку от Бафордса, округ Бедфорд, Виргиния, и не найденного до настоящего времени», хранящейся в Библиотеке Конгресса США*


THE LOCALITY OF THE VAULT

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975, 14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485, 604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225; 401, 370, 11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500, 538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283, 118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21, 24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131, 160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62, 110, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568, 614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4, 30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461, 44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 71, 216, 728, 965, 818, 2, 38, 121, 195, 14, 326; 148, 234, 18, 55, 131, 234, 361, 624, 5, 81, 623, 48, 961; 19, 25, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86, 36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985, 233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62, 194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895, 10, 6, 60, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62, 31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31, 86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 123, 216, 548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56, 216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617, 84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543, 897, 624, 18, 212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88, 612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132, 40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324, 403, 912, 227, 936, 447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323, 428, 601, 203, 124, 95, 216, 814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84, 221, 736, 820, 214, 11, 60, 760.

*Первая шифрограмма Бейла содержащая информацию о координатах клада*

форд, Виргиния, и не найденного до настоящего времени». Несмотря на широкий интерес к книге и большое число исследователей шифрограмм Бейла, многие из которых посвятили поиску разгадки всю свою жизнь, первая и третья шифрограмма до сих пор остаются неразгаданными.

## Заключение

В современном мире при широкой доступности компьютеров книжный шифр трансформировался в части используемых хранилищ данных и самого формата ключевой информации — теперь вместо бумажных книг используются файлы с информацией. Текстовые файлы, изображения, видео, аудио — неважно какие это файлы — это последовательность битов 0 и 1. Разбивая файлы на условные блоки, можно задать координаты ключа шифрования, по которым будут находиться нули и единицы, из которых можно составлять новые бинарные последовательности, определяющие новую информацию — тайное сообщение. Дешифровать такие шифры без знания ключа методически не представляется возможным.

## Упражнения

В качестве домашнего задания и самостоятельных упражнений рекомендуем выполнить следующее:

1. Прочитайте следующие художественные произведения:

• Бабаш А. В., Шанкин Г. П. История криптографии. Часть I. М.: Гелиос, 2002.

• Синельников А. В. Шифры и революционеры России

2. Расшифруйте следующее зашифрованное послание по ключевому тексту из таблицы в примере в статье: 1/4, 10/7, 9/8, 2/6, 10/2, 1/10, 4/6, 8/5, 5/9, 4/10, 3/7, 8/6, 5/9.

## Юмор Юмор Юмор Юмор Юмор Юмор

* * *

Раньше я играл в теннис, футбол, хоккей, занимался шахматами и картингом. Но всё кончилось, когда сын сломал компьютер.

* * *

Человеку свойственно ошибаться. Но для того, чтобы окончательно все испортить, требуется пароль администратора.

* * *

Если Вы видите объявление: «Продам принтер» — написанное от руки, то что-то здесь не так...