



Душкин Роман Викторович
*Директор по науке и технологиям
Агентства Искусственного Интеллекта
(roman.dushkin@gmail.com)*

Решётки Кардано

Мы продолжаем изучение основ криптографии, которое мы начали в предыдущих номерах журнала «Потенциал». На этот раз мы начнём плотное изучение блочных шифров, и на острие нашего внимания будет занятая схема шифрования, которая называется «решётка Кардано». При правильном использовании это практически не поддающийся криптоанализу метод, так что он будет интересен тем, кто хочет прятать свои секреты. Хотя, конечно, по меркам профессиональной криптографии метод является устаревшим.

Мы уже изучили большое количество систем шифрования, и некоторые из них даже обладают высокой степенью точности, причём для их использования не требуется больших усилий. Например, шифр пропорциональной замены довольно сложно взломать, хотя, в конце концов, конечно же, он тоже поддастся. Но если следовать доктрине Россиньоля, которую мы изучили в предыдущей статье цикла¹, то часто шифр пропорциональной замены помогает для оперативного обмена скрытыми посланиями – пока криптоаналитик будет разгадывать шифрограмму, её актуальность уже будет потеряна. Тем



Джероламо Кардано

¹ См. № 2 2019 г.

не менее, эта система шифрования довольно громоздка для использования, особенно если для обеспечения равномерного распределения частот в шифрограммах используется большое количество символов.

Давайте познакомимся с новой криптографической системой, которая довольно проста в использовании, но при этом очень устойчива к взлому, особенно если правильно её использовать. Речь идёт о так называемой «решётке Кардано» – одному из ранних вариантов блочного шифра. Изначальный вариант этой шифросистемы разработал известный итальянский учёный Джероламо Кардано, в честь которого названы формула Кардано для решения кубического уравнения, карданный вал, карданов подвес, и вот рассматриваемая нами решётка Кардано.

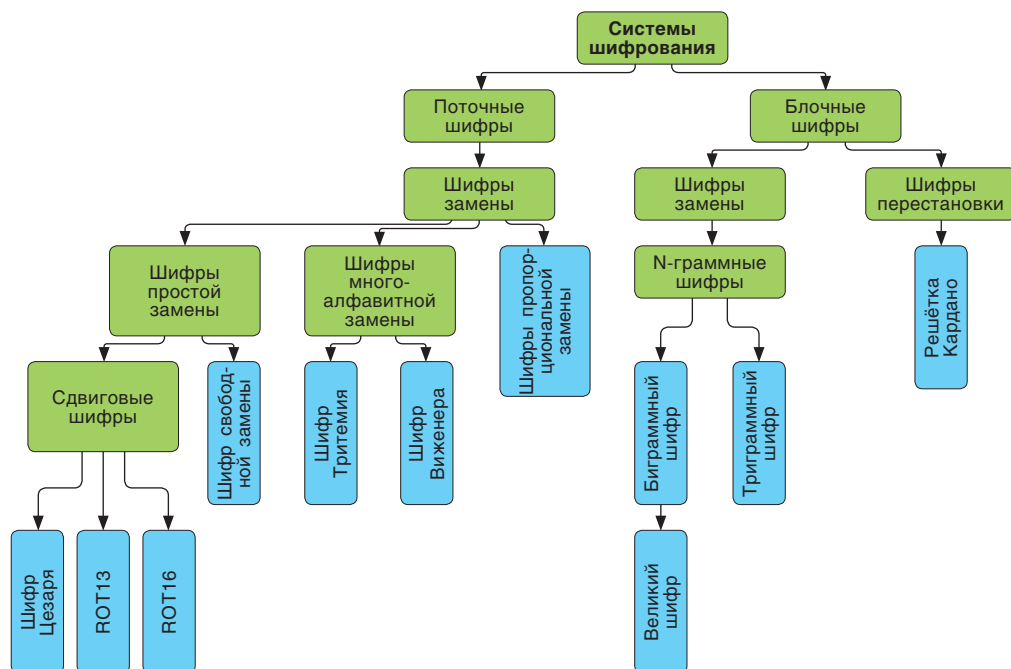
Мы уже изучали блочные шифры. Вспоминайте, блочным на-

зывается такой шифр, в котором функция шифрования применяется к блокам открытого текста фиксированной длины, а результат зависит от ключа и, возможно, результата для предыдущего блока. Практически, блокчейн.

Блокчэйн (англ. blockchain, изначально block chain) – выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию.

Википедия

Действительно, концепция блокчейна была известна криптографам задолго до публикации Сатоши Накамото своей Белой книги об организации блокчейна биткойна. Так вот N-граммные шифры можно отнести к блочным. К таковым же относится и изучаемый нами сегодня шифр Кардано. Так что обновим диаграмму систем шифрования.



Здесь надо отметить, что изначально Джероламо Кардано разработал несколько иной метод, отличающийся от того, что мы изучим здесь. Метод, который он изобрёл, относится, скорее, к стеганографии, нежели чем к криптографии.

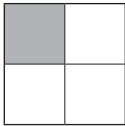
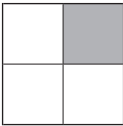
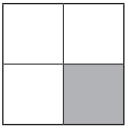
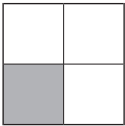
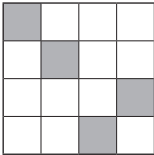
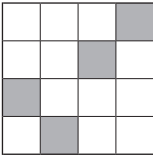
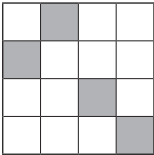
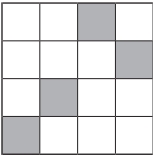
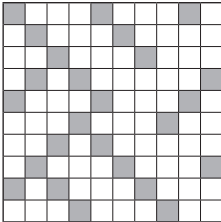
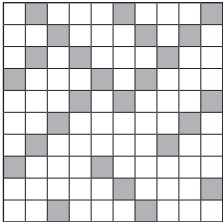
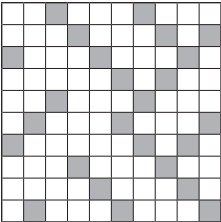
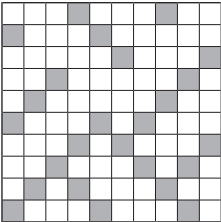
Метод шифрования

Для шифрования при помощи решётки Кардано необходимо эту самую решётку изготовить. Решётка – это квадратная матрица, размер которой чётный. Чем больше размер, тем больше символов сообщения можно зашифровать при помощи одной матрицы, и тем сложнее криптоаналитику будет её взломать. Давайте рассмотрим конкретный пример на матрице размера 10×10 ...

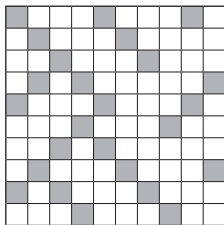
В матрице размером 10×10 имеется 100 позиций. Саму квадратную матрицу можно повернуть вокруг её центра 4 раза. Это значит,

Стеганографию, то есть науку о сокрытии самого факта передачи информации, мы оставим на потом. А сегодня изучим метод, который был разработан несколько позже, но назван именно в честь Кардано. К тому же, они очень похожи.

что среди 100 позиций надо выбрать $25 = 100/4$ «закрашенных» позиций, которые будут соответствовать тем местам, в которые записываются символы открытого текста. Эти 25 позиций надо выбрать так, чтобы при повороте матрицы на 90, 180 и 270 градусов выбранные закрашенные позиции никогда не накладывались друг на друга. И, соответственно, если совместить четыре матрицы – построенную и её же, но повернутую на 90, 180 и 270 градусов, то все 100 позиций должны быть закрашены. Например:

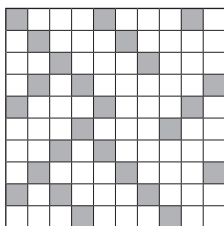
Размер матрицы	Поворот (по часовой стрелке)			
	0°	90°	180°	270°
				
				
				

Итого, например, у нас получилась вот такая матрица размера:



Можно легко убедиться, что если эту матрицу трижды повернуть на 90, 180 и 270 градусов, а потом все четыре матрицы совместить, то в получившейся матрице все поля будут закрашены, а незакрашенных позиций не будет.

Теперь давайте попробуем при помощи этой матрицы что-нибудь зашифровать. Ну, к примеру, этот вот самый текст, который вы читаете. Прямо с начала абзаца. Для этого надо начать выписывать все символы текста в закрашенные поля матрицы по порядку. Вот так:

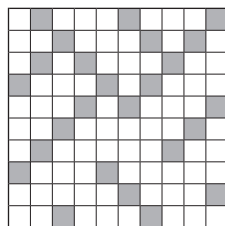


Как только первые 25 полей

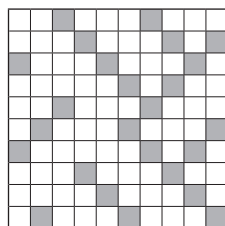
ТПЬТЕ ОЗВПМ ОЕОАТ РШШИИ ФЭЪТР
ЕНЦПК УСОЫК ПЧПТР КРТИО ООТМН

Для следующих ста букв процедура повторяется, однако лучше использовать новую матрицу. Вообще, чем больше разных матриц используется, тем устойчивее шифрограмма. Однако, конечно же, и у отправителя, и у получателя таких шифрограмм должна быть одинаковая последовательность ма-

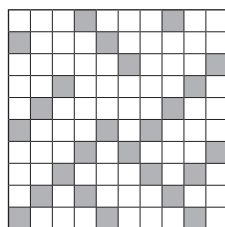
заполнены, матрица поворачивается на 90 градусов, и процесс продолжается:



Следующий поворот:



И, наконец, последний поворот:



И в итоге получается такая шифрограмма, перемешивающая первые 100 букв исходного сообщения:

СДООА ЙАМВМ ВААЫА ЙЙТТТ РЪТЕИ
БОЕРУ ЕЫМЙР ИПВУВ ЫЗУРЧ ТДИИО

триц, которые используются для шифровки и расшифровки.

Также необходимо отметить, что если конец текста, который подлежит шифрованию, оставляет в последней матрице незаполненные позиции, то их необходимо заполнить случайными символами, чтобы обеспечить секретность.

Само собой разумеется, что крайне желательно, чтобы распределение частот этих случайных символов

совпадало с таковым распределением букв того языка, сообщение на котором шифруется.

Методы атаки

Давайте теперь подумаем, какими методами может воспользоваться криптоаналитик для дешифровки шифрограммы, смысл которой скрыт при помощи решётки Кардано. Как обычно, необходимо решить следующие задачи:

1. Определить тип шифра, то есть в рассматриваемом случае — определить, что это действительно шифр Кардано.
2. Определить параметры шифрования. В рассматриваемом случае — размеры использованных решёток и их количество.
3. Собственно, дешифровать сообщение.

С решётками Кардано есть проблема — очень сложно понять, что шифрограмма построена на их основе. Перемешивание символов исходного текста не меняет частотность символов. Но вот такие намёки могут дать подсказку:

1. Если в шифрограмме используются те же самые символы, что и символы открытого текста (это очень слабый намёк).
2. Если в шифрограмме частотность символов абсолютно такая же, как и частотность открытых текстов на заданном языке, но при этом разгадать шифрограмму методом частотного анализа не представляется возможным.
3. Если в шифрограмме часто встречаются последовательности одинаковых букв, стоящих вместе, то в совокупности с неизменённой частотностью

это, скорее всего, намекает, что перед криптоаналитиком перестановочный шифр.

4. Наконец, если количество символов в шифрограмме можно выразить как kn^2 , то есть как целое число квадратов, то это очень сильный намёк на использование решёток Кардано.

Если получена шифрограмма, которая так или иначе совпадает с перечисленными четырьмя критериями (особенно с четвёртым), то можно предположить, что перед нами шифрограмма, зашифрованная при помощи решёток Кардано. Но что делать дальше? А дальше, кроме как методом подбора, вряд ли что-то получится сделать.

Давайте посмотрим, как можно осуществить перебор. Для квадратной матрицы со стороны $(2m)^2$ необходимо выбрать $(2m)^{2/4} = m^2$ закрашенных позиций. Комбинаторика даёт нам ответ — это число сочетаний из $(2m)^2$ по m^2 , то есть:

$$C_{2m^2}^{m^2} = \frac{(4m^2)!}{m^2! (4m^2 - m^2)!} = \frac{(4m^2)!}{m^2! (3m^2)!}.$$

Это довольно большое число при возрастающем m . Его, конечно ещё надо разделить на 4, так как не требуются сочетания, переводимые друг в друга поворотами. Но тем не менее. Чтобы понять проблему, давайте посмотрим, чем равно это число для m от 1 до 5, что соответствует матрицам Кардано с чётными сторонами от 2 до 10:

	1	2	3	4	5
	4	1 820	94 143 280	$4.89 \cdot 10^{14}$	$2.43 \cdot 10^{23}$

Ну вот это и называется комбинаторным взрывом. Если бы у нас был компьютер, который мог бы изучать миллиард комбинаций в секунду (примерно так могут сегодня работать современные суперкомпьютеры), то перебор всех вариантов для решётки 10×10 занял бы более 461 миллиона лет.

Так что для полного перебора решёток Кардано с размером 10×10 и выше у нас просто нет вычислительных ресурсов. И даже появление универсальных квантовых компьютеров не очень-то и поможет, так как рост размерности рассматриваемой нами сейчас задачи является факториальным, а квантовые компьютеры смогут помочь только с экспонен-

циальными задачами. А задачи с факториальной сложностью являются ещё более сложными, чем задачи с экспоненциальной. Как быть?

К сожалению, ответ на этот вопрос одновременно и банальный, и малообнадёживающий. Единственная возможность для криптоаналитика взломать перестановку символов в открытом тексте при помощи матриц Кардано – это так или иначе получить эти матрицы. Существует много способов, многие из которых выходят за рамки обычного арсенала криптоанализа. Однако при помощи методов социальной инженерии это вполне возможно. Но это уже совсем другая история.

Заключение

Итак, мы изучили ещё один метод блочного шифрования, который довольно простой, и при этом стоек к взлому. Как видно на этом примере, старые и простые криптографические системы не обязательно являются плохими или ненадёжными. Но сегодня я вряд ли рекомендовал бы

пользоваться только этим методом, хотя для быстрых нужд при наличии большого набора готовых решёток он вполне подходит. Потренируйтесь использовать этот метод в своей практике. В любом случае, это пригодится для будущего, когда мы будем изучать каскадное шифрование.

Упражнения

В качестве домашнего задания и самостоятельных упражнений рекомендую выполнить следующее:

1. Прочитайте следующие художественные произведения:
 - Яценко В. В., Дориченко С. А.

- 25 этюдов о шифрах: популярно о современной криптографии.
2. Напишите на своём любимом языке программирования программу, которая получает на вход размер решётки Кардано, а возвращает список возмож-

ных решёток Кардано этого размера. Должна быть возможность выбрать из этого списка определённую решётку и по-

BAOMЛ	ЕШЭКТ	ЕОГЙН	ЛСЕТЬ	КАНТВ	ЛАНОТ	ЮОБЕЙ	ЧИЗСЭ	АКТЛР	ОАГОВ
АОДРК	НИЗОГ	ИАЗДП	ЗЕАРК	ВЭСТЛ	ООГЛВ	ООЮЕЧ	АСЦХА	ИПЛКЕ	ОЛОДТ
АСВСК	СТОЯЭ	ВААТЗ	ТКЕАЙ	ХДОВА	УНЧДА	УГЩРИ	ВВЭРТ	АОАСМ	ХМКМШ
РЦИАИ	ФИКВР	ЛПОТЕ	ВТДКО	ЕОРГО	АРРХЗ	САЛЙЕ	ЕАИМЩ	МИ	

Если известно, что, во-первых, используется только одна решётка Кардано, но для каждого следующего блока текста она может начинаться в любой позиции; во-вторых, в каждом квадранте ре-

лучить её визуализацию для дальнейшей распечатки.

3. Расшифруйте следующую шифрограмму:

шётки Кардано есть только ровно и 25 % вырезанных позиций от общего числа вырезанных позиций всей решётки; в-третьих, никакие две вырезанные позиции не граничат друг с другом стороной.