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

Великий шифр

Мы продолжаем наше увлекательное путешествие в страну криптографии, и в этой статье погрузимся в историю развития науки о шифрах и сокрытии информации. Одним из наиболее сложных шифров, который использовался в древности, был так называемый «Великий шифр», разработанный Антуаном Россиньолем, первым профессиональным криптоаналитиком Франции, работавшим в Чёрном кабинете. Этот шифр был недоступен для взлома на протяжении двух веков.

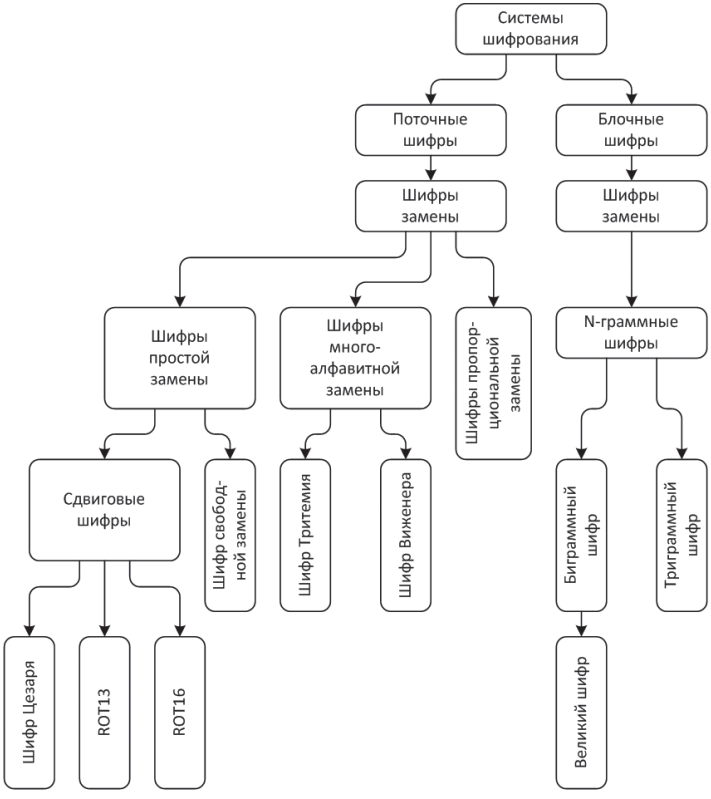
Криптография как наука начала своё шествие по миру после того, как были получены первые достижения криптоанализа. Криптоанализ как наука стал шествовать по миру после того, как различные страны и правители начали использовать более сложные и замысловатые шифры по сравнению с шифром простой подстановки. И до сих пор эти два направления идут бок о бок, показывая своеобразную «гонку вооружений» и определённого рода «естественный отбор». Эти биологические термины использованы не зря – криптографы стремятся защитить секреты, а криптоаналитики пытаются эти секреты выведать, взломав шифры. И те, и другие создают друг для друга давление отбора, как травоядные и хищники в природе. И если криптограф делает шифр, который невозможно взломать существующими методами, криптоаналитику приходится разрабатывать новые методы, которые рано или поздно помогут взломать шифр, что приведёт к тому, что криптографу придётся придумывать новый шифр. И так по кругу до бесконечности...

И вот во Франции в XVII веке вместе с возникновением регулярной почтовой службы появляется так называемый «Чёрный кабинет». Это орган, в котором специально обученные сотрудники занимались вскрытием переписки и её дешифровкой в случае использования тайнописи. В 1628 году гениальный молодой человек Антуан Россиньоль, занимавший тогда неприметную должность, расшифровывает письма из осаждённой

крепости Ла-Рошель. После этого он становится первым профессиональным криптоаналитиком Франции. Он основал целую династию криптоаналитиков, так как после него руководителями Чёрного кабинета во Франции были его сын и внук.

Так что Антуан Россиньоль, обладая практически полным знаниям о применявшихся в его время системах шифрования и методах их взлома, решает создать шифр, который был бы устойчив к существующим методам. В результате появился так называемый «Великий шифр», который получил репутацию невзламываемого и применялся до XIX века, а потом до 1890 года все шифровки, выполненные этим шифром и его модификациями, превратились для историков в нечитаемый набор цифр.

Сам по себе шифр Россиньоля представляет собой N-граммный шифр (N = 2, то есть шифр биграммный) с некоторыми модификациями. Так что можно обновить нашу диаграмму с классификацией шифровальных систем следующим образом:



Метод шифрования

В оригинальном Великом шифре использовался набор из 587 чисел, большая часть из которых представляли слоги французского языка. Но были числа и иного рода. Некоторые шифровали одну букву, причём для наиболее частых букв использовалось несколько вариантов, иные – целое слово. И были числа, которые, например, отменяли предыдущее число. Всё это было предназначено для борьбы с частотным анализом, которым Антуан Россиньоль сам владел в совершенстве. Итого Великий шифр сочетал в себе свойства следующих систем шифрования:

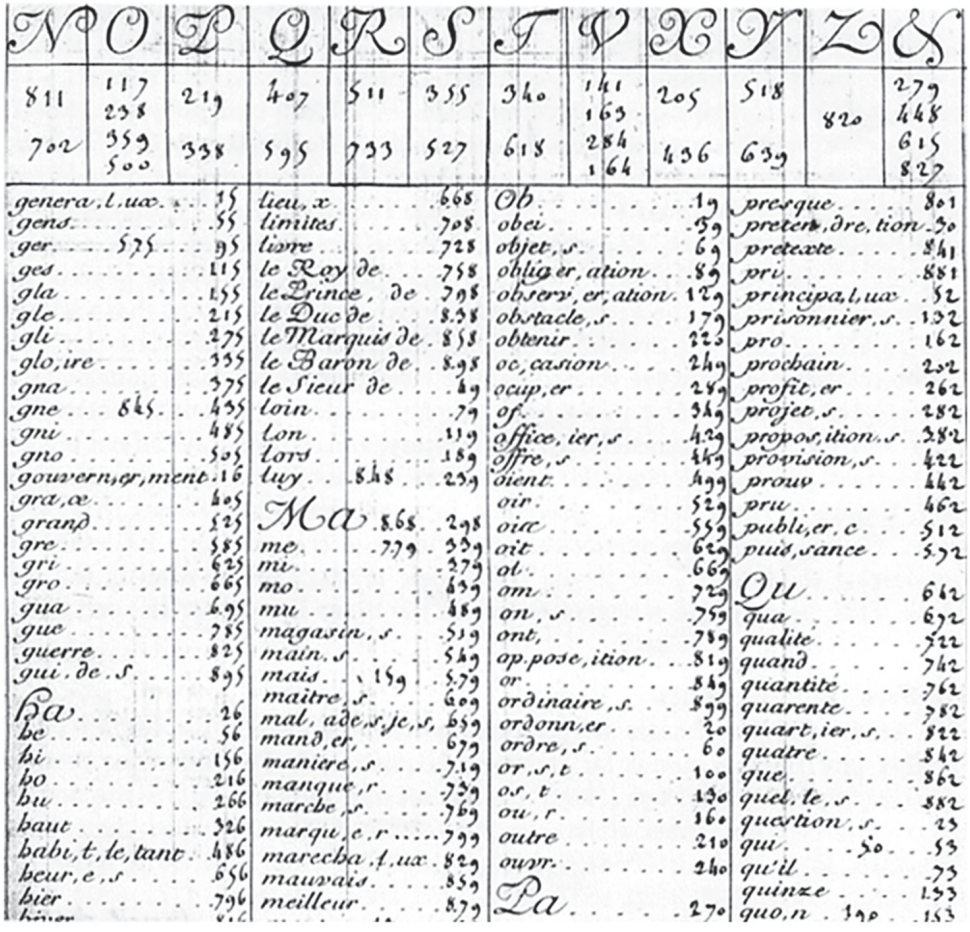
1. Шифры замены (замена слогов, в основном биграмм).

2. Пропорциональный шифр (только для наиболее часто встречающихся букв и слогов).

3. Номенклаторы (замена целых понятий).

4. Использование операторов (числа, меняющие смысл других чисел).

Вот так выглядела одна из страниц, позволяющая осуществлять шифрование и расшифровку при помощи Великого шифра:



На этой иллюстрации видно, что шифр, скорее, не биграммный, а шифрует слоги, хотя многие из них и состоят из двух букв. Но иногда попадаются числа, которые шифруют целые слова, как полагается, наиболее часто встречающиеся в том тексте, для которого предназначен этот шифр (то есть в старые времена – для дипломатической и военной переписки). Так что действительно, криптоаналитики всей Европы того времени ломали себе головы, но так и не смогли подступиться к этому шифру.

Давайте подумаем, как можно было бы сделать аналог Великого шифра для русского языка. Для этого необходимо:

1. Для каждой буквы русского алфавита выбрать определённое количество чисел, пропорциональ-ное частоте буквы.

2. Составить список всех возможных слогов русского языка (или, хотя бы, открытых слогов, состоящих из двух букв – «БА», «РО», «ЖУ» и т.д. – и закрытых слогов, состоящих из трёх букв – «МОЙ», «ТЕН», «ДУЛ» и т. д.) и каждому из них приписать число, а для пары десятков наиболее часто встречающихся слогов приписать по два числа.

3. Составить список из пары десятков наиболее часто встречающихся слов (или корней) русского языка и каждому из них приписать по одному числу.

Подумайте, зачем требовался такой мощный и стойкий к криптоанализу того времени шифр? Ведь затраты времени на шифрование и расшифровку текстов при помощи Великого шифра несопоставимы с теми же шифрами простой подстановки, в которых можно либо пользоваться простой формулой, либо просто запомнить три десятка значков, как это делали мы в детстве. И процесс сокрытия информации будет так же быстр, как и написание той же информации в открытом виде. А вот Великий шифр так просто не запомнить, если там сотни разных символов для разных слогов и даже некоторых часто встречающихся слов. Конечно, чем чаще им пользоваться, тем будет проще, и опыт китайского языка это подтверждает, но поначалу как шифрование, так и расшифровка будут довольно длительными. Ради чего?

Всё дело в так называемой «доктрине Россиньоля». Антуан Россиньоль разработал принцип, согласно которому стойкость шифра, используемого для военных целей, должна быть достаточной для обеспечения секретностисообщения до получения его армейским подразделением и выполнения приказа. А вот дипломатический шифр должен быть таким, чтобы его раскрытие заняло несколько десятков, а может быть, и сотен лет, так как в дипломатии зашифрованный документ часто должен оставаться секретным ещё очень продолжительное время после его зашифровки.

Именно это и побудило Россиньоля создать Великий шифр.

Метод атаки

Как уже сказано, Великий шифр Россиньоля успешно использовался криптографами Франции, и взломать его не могли в течение двух веков. Потом постепенно он вышел из употребления, его номенклатуры забылись и потерялись, и историкам досталась кипа зашифрованных писем, которые больше нельзя было прочитать без дешифровки. Но письма эти были крайне интересны именно с исторической точки зрения, так как могли пролить свет на многие события тех времён.

Историки долго и безуспешно бились над Великим шифром, пока в 1890 году письма, зашифрованным им, не попали к Этьену Базери, который работал в отделе шифрования французской армии. Он в течение примерно года смог расшифровать эти письма, проверив и отвергнув множество гипотез и наконец, найдя ту самую ниточку, потянув за которую он смог распутать двухсотлетнюю тайну.

Этьен Базери начал, как полагается, с подсчёта частот. Но он резонно предположил, что раз символов в Великом шифре более пятисот, то это либо номенклатор, либо шифр пропорциональной замены. Но подсчёт частот используемых в письмах чисел ничего не дал – корпус шифрограмм был слишком мал. Несколько месяцев криптоаналитик комбинировал частоты и пытался найти подсказки, но всё было тщетно. Через какое-то количество попыток он решил отказаться от идеи о том, что это шифр пропорциональной замены.

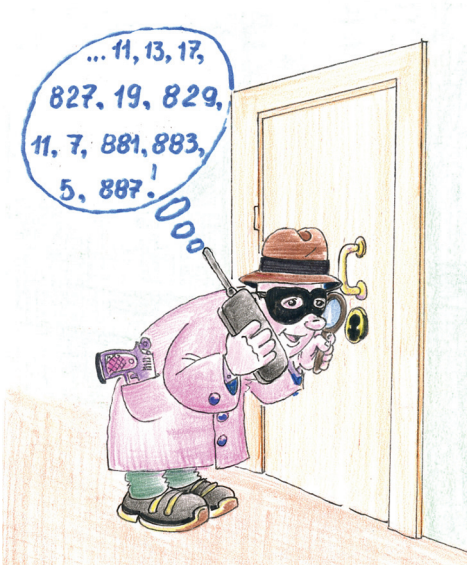
Следующая гипотеза, которую начал проверять Этьен Базери, заключалась в том, что числа шифруют двойки букв. Другими словами, он предположил, что Великий шифр является биграммным. Ведь во французском алфавите 26 букв, если не считать букв с диакритическими знаками, а, следовательно, биграмм может быть 676 штук. Принимая во внимание то, что некоторые биграммы не существуют во французском языке, можно с уверенностью сказать, что гипотеза имеет право на существование. Соответственно, криптоаналитик начал частотный анализ по биграммам. Но у него опять ничего не вышло.

Третья гипотеза, к которой перешёл мсье Базери, заключалась в том, что каждое число соответствует одному слогу во французском языке. И тут криптоаналитик был совсем близок к истине, но у него всё равно ничего не получалось. Частотный анализ слогов результатов тоже не давал, и это, скорее всего, происходило из-за наличия в шифрограммах чисел-операторов. Но он не сдавался, и в какой-то момент начал строить предположения о том, какие слоги могли бы скрываться за повторяющимися последовательностями в наиболее часто встречающихся словах. Одним из таких слов было 124-22-125-46-345, которое появлялось очень часто – практически на каждой странице. Ба-зери предположил, что это слово «les-en-ne-mi-s», то есть «враги». И это было тем криптоаналитическим прозрением, которое обычно даёт первую ниточку, помогающую распутать весь клубок.

Собственно, это и послужило началом полной дешифрации Великого шифра. Артикль «les» встречается во французских текстах довольно

часто. После этого предположения криптоаналитику пришлось только лишь скрупулёзно отыскивать другие появляющиеся в процессе криптоанализа зацепки и тщательно их распутывать. Фактически, атака на шифр была произведена изначально при помощи подбора ключевых слов, а только потом был применён частотный криптоанализ на уровне слогов. И числа-операторы тут уже не помогли, поскольку их было слишком мало, и они не могли существенно запутать текст.

Вот здесь надо особенно обратить внимание на то, что у любого криптоаналитика всегда остаётся возможность подбора. Всегда надо помнить, что каким бы сложным шифр ни был, но если он основан на каких-то закономерностях, то криптоаналитик может взломать его при помощи догадок о тех или иных встречающихся в тексте словах. Для этого надо всегда размышлять о том, кто кому и по какому поводу посылает шифрограмму, и уже эта информация может дать очень много подсказок. Слово «враги» с очевидностью могло многократно присутствовать в дипломатической переписке Французского двора, чем и воспользовался удачливый Этьен Базери. Впрочем, ему повезло...



5 мая 1921 года была создана криптографическая служба России, по постановлению Совета народных комиссаров РСФСР. Эта дата считается днем рождения криптографической службы, её часто называют днем шифровальщика.

В списке профессиональных праздников России есть еще одна дата – **13 ноября**, которую тоже отмечают как день шифровальщика. По распоряжению Ленина приказом Реввоенсовета № 217 от 13.11.1918 года было создано «Шифровальное отделение Отчетно-организационного отдела Организационного управления Всероссийского Главного штаба».

Заключение

Итак, Великий шифр продержался два столетия и успешно выполнял роль дипломатического шифра Франции. Он был основан на правильном понимании принципов криптографии и, главное, предвосхищении того, какими методами будут пользоваться криптоаналитики того времени для атаки на шифрограммы. Сегодня, конечно же, он не выстоял бы перед переборной силой современных компьютеров, но взломал его

криптоаналитик, применивший нестандартное мышление. Он не пользовался вычислительной техникой (её тогда просто не было), он умело воспользовался своей интуицией.

В следующей статье цикла мы изучим перестановочные шифры и один из самых известных вариантов – решётки Кардано. Оставайтесь с нами.

Упражнения

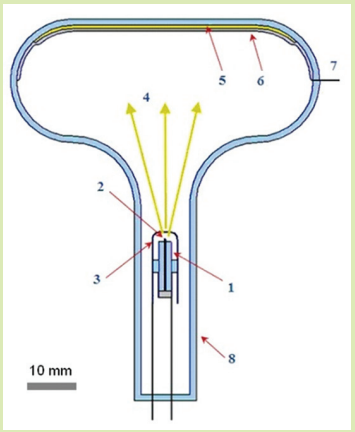
В качестве домашнего задания и самостоятельных упражнений рекомендую выполнить следующее:

1. Прочитайте следующие художественные произведения:
Стивенсон Н. *Барочный цикл.*
2. Составьте свой вариант аналога Великого шифра для русского языка.
3. Обратитесь по адресу https://goo.gl/Af7keT, чтобы найти пятое волшебное слово.
4. На своём любимом языке программирования составьте программу для зашифровки и расшифровки сообщений при помощи заданного варианта Великого шифра.

Калейдоскоп Калейдоскоп Калейдоскоп

Лампочка Шешина будет конкурировать со светодиодами

Сотрудники кафедры вакуумной электроники МФТИ совместно с учеными из ФИАН создали и испытали прототип катодолюминесцентной лампы общего освещения, основанной на явлении автоэлектронной эмиссии и обладающей не достигнутыми никем в мире характеристиками надежности, долговечности и силы света. Соответствующая работа опубликована в международном научном журнале Journal of Vacuum Science & Technology B.



Ставшие уже привычными в быту светодиодные лампочки – не единственная экономичная альтернатива лампам накаливания: с 1980-х годов в мире изучают возможность применения для общего освещения так называемых катодолюминесцентных светильников. Их работа основана на том же принципе, что и кинескопы старых телевизоров: внутри вакуумной колбы находятся катод (отрицательный электрод) и анод (положительный электрод), между которыми создается значительная разность потенциалов (до десятка киловольт). Под действием электрического поля электроны, испускаемые катодом, бомбардируют поверхность анода, под которой нанесен слой люминофора, и заставляют последний светиться.

Схема устройства лампочки: 1 – модуль катодного модулятора; 2 – катод; 3 – модулятор; 4 – испускаемые электроны; 5 – люминофор; 6 – анод (алюминиевое зеркало); 7 – вывод анода; 8 – стеклянная вакуумная колба

https://mipt.ru/news/lampochka_sheshina_budet_konkurirovat_so_svetodiodami