

Михаил Масленников

Занимательная криптография. Часть 2.

18+

Михаил Масленников

**Занимательная
криптография. Часть 2.**

«Автор»

2026

Масленников М. Е.

Занимательная криптография. Часть 2. / М. Е. Масленников —
«Автор», 2026

Я решил попробовать изложить некоторые современные понятия криптографии на простом и понятном языке неискушенному читателю, популяризировать криптографию. Криптография – это один из разделов математики, поэтому при ее популяризации не обойтись без математических выкладок с математическими понятиями и формулами, которые могут быть непонятны рядовому читателю. Я, как мог, постарался объяснить их на простом житейском языке, частенько прибегая к различным выдумкам и фантазиям. Надеюсь, что получилась занимательная криптография, которая может быть полезной широкому кругу читателей.

© Масленников М. Е., 2026

© Автор, 2026

Содержание

Их покупают.	5
Нежеланный ребенок.	11
Конец ознакомительного фрагмента.	12

Михаил Масленников

Занимательная криптография. Часть 2.

Их покупают.

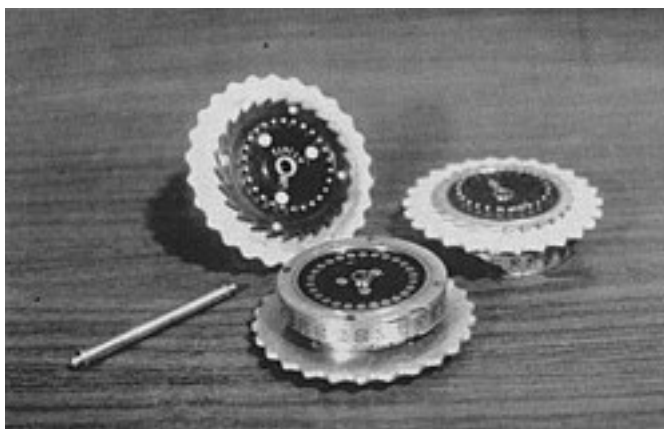
1975 год. На 4 факультете Высшей Краснознаменной школы КГБ СССР идет лекция по СД-7А – спецдисциплине 7 (криптография) А (основы). Лектор – Борис Петрович Антонов, криптограф старой закалки, - рассказывает про дисковые шифраторы и методы их криптографического анализа. Ключи у таких шифраторов бывают двух типов: долговременные и разовые. Долговременные – это коммутации движущихся дисков, а разовые – их начальные угловые положения.

Разовые ключи могут быть определены с помощью типовых криптографических приемов – протяжки некоторых вероятных слов в шифртелеграмме, опробованием допустимых вариантов, согласованием и т.п.

- А долговременные ключи никто не опробует. Их покупают.

А где покупают? Наверное, в «военторге». Там, если верить некоторым политикам, можно многое чего купить.

Если читатель собирается в «военторг», то могу подсказать, как выглядят эти долговременные ключи, чтобы легче было их искать на прилавках.



Здесь и далее - картинки из Википедии: <https://ru.wikipedia.org/wiki/%D0%AD%D0%BD%D0%B8%D0%B3%D0%BC%D0%B0>

Это – только присказка к сказке про дисковые шифраторы. А теперь – сама сказка.

В начале XIX века в Европе началась промышленная революция. Помните главу про то, как Суворов дешифровывал простую замену? Не могу ручаться за 100% достоверность этих сведений, но в 1794 году промышленная революция до России еще не добралась. Может быть, действительно Екатерина Великая заставляла своих полководцев шифровать донесения с помощью простой замены, но если это и было, то, в основном, с целью приучить вольных гусар к немецкому порядку и дисциплине. К тому же большинство солдат и крестьян России того времени были неграмотными, так что такой защиты во многих случаях было достаточно.

Не было еще в 1794 году ни компьютеров, ни Интернета, ни StarLink, ни даже обычной печатной машинки. Писали гусиными перьями – вспомните Пушкина. И как писали!

Читаем в Википедии.

«Примерно в 1808 году Пеллегрини Турри (Pellegrino Turri), также известный как изобретатель копировальной бумаги, создаёт собственную печатную машинку.»

Гусиные перья – хорошо, а печатная машинка – лучше. Но психология ненасытной пушкинской старухи пошла дальше.

Простая печатная машинка – хорошо, а машинка, которая будет одновременно и печатать, и шифровать – еще лучше. А точнее – и шифровать, и печатать, ибо шифрование должно быть первым.

Читаем в Википедии.

«Эни́гма» (от нем. Enigma — загадка) — переносная шифровальная машина, использовавшаяся для шифрования и расшифрования секретных сообщений. Первую версию роторной шифровальной машины запатентовал в 1918 году Артур Шербиус. На основе конструкции первоначальной модели «Энигмы» было создано целое семейство электромеханических роторных машин под тем же названием, применявшихся с 1920-х годов в сфере коммерческой и военной связи во многих странах мира, но наибольшее распространение получили в гитлеровской Германии во время Второй мировой войны. Именно германская военная модель чаще всего подразумевается при упоминании «Энигмы».

«Энигма» является настолько хрестоматийным устройством в криптографии, что есть смысл поговорить о ней поподробнее.

В алгебре есть такое понятие, как подстановка. Это такая табличка, по которой происходит простая замена символов некоторого алфавита A или, говоря более строгим математическим языком, взаимно-однозначное отображение алфавита в себя. Подстановка обозначается как P , $P(a) = b$, $a, b \in A$.

Под произведением подстановок P_1 и P_2 понимается их последовательное применение:

$$P_1 * P_2(a) = P_2(P_1(a))$$

С простой заменой мы уже встречались в книге 1. В «Энигме» же простыми заменами, причем различными, были коммутации движущихся дисков. В роли алфавита выступали 26 букв латинского алфавита от A до Z .

Если у нас есть некоторый алфавит из N символов, то множество всевозможных различных подстановок этого алфавита вместе с описанной выше операцией умножения подстановок называется симметрической группой и обозначается как S_N . Операция умножения подстановок в большинстве случаев не является коммутативной, т.е. легко найти такую пару подстановок P_1 и P_2 , для которой

$$P_1 * P_2 \neq P_2 * P_1$$

Таким образом, группа S_N не является абелевой. Помним генерала из анекдота про ЕСС?

Каждый диск на приведенной выше картинке фактически и является механической реализацией некоторой подстановки шифруемого алфавита A . Если предположить, что алфавит A содержит N символов, то на диске N контактов с внешней стороны, и N – с внутренней. Давайте лучше будем называть внутреннюю сторону каждого диска входом, а внешнюю – выходом. Какую сторону считать внешней, а какую – внутренней – спросите об этом у немца Шербиуса. Математикам до этого дела нет. Нам также нет дела и до того, какими символами обозначать на диске буквы алфавита A : русскими, латинскими, пляшущими человечками с флажками, как у Шерлока Холмса или еще как. Будем обозначать их цифрами по числу букв в алфавите. Для латинского алфавита это 1, 2, ..., 26. Давайте договоримся, что 1 – это A .

Картинки любят все. Это внутренняя и внешняя стороны диска.



Контакты соединены между собой проводами или, на криптографическом языке, перепайками.

Палочка на первой картинке – это ось, на которую насаживаются диски. Контакты дисков, насаженных на ось, соприкасаются друг с другом.

Насадиле диски на ось, контакты касаются, как шифровать будем? Гусиным пером? Нет, с помощью цивилизованной (почти!) клавиатуры, под которую запрячем эти товары из «воен-торга».



Простые печатные машинки бывают чисто механическими, а бывают электромеханические. Энигма же – это только электромеханическая машина. При каждом нажатии на клавишу клавиатуры на вход определенного контакта первого диска подавался электрический импульс. Он проходил через все три диска и появлялся на одном из контактов на выходе третьего диска. В зависимости от контакта на выходе загоралась соответствующая лампочка этого чуда техники. Рычаг с буквой и печать через ленту, как в обычной печатающей машинке? Нету! Берите гусиное перо и записывайте, какие лампочки зажигаются. По крайней мере, так было в первых версиях «Энигм». Так и до бунта недалеко. Но... (читаем в Википедии)

«Удобной деталью, использовавшейся на «Энигме» модели «М4», был так называемый «Schreibtafel», маленькое печатающее устройство, которое могло печатать все 26 букв на небольшом листе бумаги. В связи с этим не было необходимости в дополнительном операторе, следящем за лампочками и записывающем буквы.»

Пора вспомнить и о математике. Что такое несколько дисков, насаженных на палочку так, что их контакты соприкасаются? Так это же произведение подстановок, описанное чуть выше!

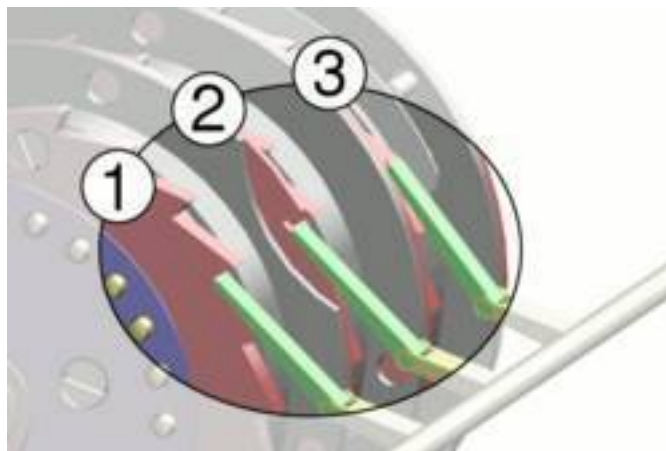
Путь P_1 , P_2 и P_3 – три подстановки на алфавите A . Насаживаем их на палочку, контакты касаются, получаем итоговую подстановку

$$P = P_1 P_2 P_3$$

Запикиваем эту палочку с насаженными на нее тремя дисками под древний-предревний keyboard с проводками и лампочками. Через статичные разъемы подключаем проводки от клавиш keyboard к динамичным входящим контактам первого диска, а проводки от лампочек – к динамичным выходящим контактам последнего, третьего диска. Все, можно шифровать?

Нет, пока еще нельзя. Точнее, можно, но не нужно. Если динамичные диски останутся статичными, то итоговый шифр будет тривиальной простой заменой, которая элементарно дешифровывается. Вся «изюминка» изобретения немца Шербиуса в том, что каждое нажатие

на клавишу древнего keyboard не только посылает электрический импульс на диски, но и обеспечивает их некоторое смещение друг относительно друга. Обеспечивает чисто механически, с помощью хвостатых собачек.



«Ступенчатое движение роторов «Энигмы». Все три собачки (обозначены зелёным) движутся одновременно. Храповик (красный) первого ротора (1) всегда зацеплён, и он поворачивается при каждом нажатии клавиши. В данном случае выемка на первом роторе позволяет собачке зацепить и второй ротор (2), он повернётся при следующем нажатии клавиши. Третий ротор (3) не зацеплен, так как собачка третьего ротора не попала в выемку второго, собачка будет просто скользить по поверхности диска»

Что дает движение диска? Предположим, что перед началом шифрования первый диск был установлен так, что контакт буквы 'А' от клавиатуры приходился на контакт 1 первого диска и позиция контакта 1 остальных двух дисков была такой же. При нажатии клавиши 'А' после зашифрования буквы 'А' первый диск поворачивается на один контакт и контакт буквы 'А' будет приходиться на контакт 2 первого диска. Это означает, что итоговая подстановка для шифрования первой буквы была

$$P^{(1)} = P_1 P_2 P_3$$

а для шифрования второй буквы секретного сообщения будет

$$P^{(2)} = X_1 P_1 P_2 P_3$$

где X_i – подстановка смещения на i шагов вида

$$X_i(y) = y + i \pmod{N}$$

Таким образом, злые собачки «Энигмы» принудительно запикивают подстановки смещения в произведение подстановок P_1 , P_2 и P_3 . Симметрическая группа S_N не является абелевой, поэтому эти «собачьи» иксы портят статистику текста и всякие СЕНОВАЛИТРы, с помощью которых легко дешифровывалась простая замена.

А где же ключи, обеспечивающие стойкость? Все просто. К «собачьим» иксам добавляем «человеческие» иксы – начальную установку положений дисков. Выше для простоты объяснений мы предполагали, что перед началом шифрования контакт с номером 1 у всех трех дисков был установлен одинаково. А если перед началом шифрования повернуть каждый из трех дисков на секретные ключевые сдвиги, то появляются «человеческие» иксы, к которым затем добавляются еще и «собачьи».

Вот таким образом немец Шербиус избавился от простой замены и сделал шифр гораздо лучший, чем практически все известные шифры того времени. Но только того времени, начала XX века. Ведь если «купить» роторные диски «Энигмы», то стойкость будет держаться только

на «человеческих» иксах, а это в общей сложности $26^3 = 17\,576$ вариантов. Чуть ли не руками можно все перебрать! А в реальной жизни так много различных «военторгов»!

Сведения из Интернета (<https://picturehistory.livejournal.com/616295.html>) о том, как покупались ключи.

«Главный улов был сделан 8 мая 1941 г. при захвате подлодки U-110 капитан-лейтенанта Юлиуса Лемпа, атаковавшего конвой OB-318. Отбомбившись по U-110, суда охранения заставили ее всплыть. Капитан эсминца HMS Bulldog пошел на таран, но, увидев, что немцы в панике прыгают за борт, вовремя отвернул. Проникнув в полузатопленную лодку, штурмовая группа обнаружила, что команда даже не пыталась уничтожить секретные средства связи. В это время другой корабль поднял из воды выживших немцев и запер их в трюме, чтобы скрыть происходящее. Это было очень важно.

На U-110 взяли: исправную «Энигму М3», комплект роторов, ключи на апрель-июнь, инструкции по шифрованию, радиограммы, журналы (личного состава, навигационный, сигнальный, радиопереговоров), морские карты, схемы минных полей в Северном море и у побережья Франции, инструкцию по эксплуатации лодок типа IXB. Добычу сравнили с победой в Трафальгарской битве, эксперты назвали ее «даром небес». Награды морякам вручал сам король Георг VI: «Вы достойны большего, но сейчас я не могу этого сделать» (через систему награждений немецкая агентура могла бы выйти на факт потери машины). Со всех была взята подписка, захват U-110 не разглашался до 1958 года.

Выпотрошенную лодку утопили ради сохранения секретности. Капитан Лемп погиб. Допрос остальных немцев выявил, что они не знают об утрате секрета. На всякий случай были приняты меры по дезинформации, при пленных сетовали и сожалели: «Высадиться на лодку не удалось, она внезапно затонула». Ради секретности даже закодировали ее захват: «Операция Примула». Потрясенный успехом, первый морской лорд Паунд радировал: «Сердечно поздравляю. Ваш цветок редкостной красоты».

Нежеланный ребенок.

С «Энигмой» во второй мировой войне немцы, честно говоря, опростоволосились. Видимо, не было у них еще чисто математического подхода к криптографии. «Энигма» выглядела внешне солидно, надежно и, видимо, у немцев не возникало желаний посмотреть на нее критически, с позиции формального математика. Получить для нее чисто математические формальные оценки стойкости в различных условиях, а затем уже оценивать, насколько эти условия реальны при повседневной эксплуатации «Энигмы».

- А что будет, если коммутации дисков станут известны противнику? Какова будет в таких условиях оценка стойкости «Энигмы»?

- Что может быть известно противнику о характере секретных сообщений, шифруемых с помощью «Энигмы»? О наличии в таких сообщениях некоторых стандартов и их местоположениях?

- Какие могут возникать типовые ошибки операторов при работе с «Энигмой»? К каким последствиям они могут привести?

Скорее всего, немцы также не учли возможности появления и использования в криптографии первых ЭВМ. В результате всех этих просчетов англичане успешно дешифровывали секретную переписку, обрабатываемую с помощью «Энигмы», что существенно влияло на ход второй мировой войны.

После войны подход к криптографии во многом изменился. Вместо «исследований», проводившихся криптографами типа Шерлока Холмса, (*«Пляшущие человечки оказались шифром простой замены с флагами — разделителями слов. Шерлок Холмс, проанализировавший ранее 160 различных шифров, взломал шифр методом атаки на основе подобранного открытого текста.»* -

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.