Всероссийский заочный конкурс исследовательских работ

«Шаги в науку»

Направление: математика

Тема: Возможности криптографии в Древнем мире

Боревич Андрей Алексеевич
ГБОУ гимназия № 73 «Ломоносовская гимназия» Выборгского района г. Санкт-Петербурга
5 класс

Научный руководитель:
Боревич Ирина Сергеевна

г. Обнинск, 2013/2014 учебный год

Оглавление

Введение

В этой работе рассказывается о возможностях наиболее известных шифров древности, которые активно использовались в то время, и тем самым заложили основы современной криптографии, включая азбуку Морзе, двоичный код, шестнадцатеричный код, и, как ни странно, даже десятичную систему счисления.

Возникла криптография почти одновременно с письменностью. Люди издавна хотели, чтобы их переписка была понятной лишь узкому кругу лиц. В то же время, люди, желающие проникнуть в тайны этой переписки, старались найти способы ее расшифровки.

У меня интерес к этой теме возник вместе с интересом к произведениям «Золотой жук» Эдгара По и «Пляшущие человечки» Артура Конан-Дойла, в которых персонажи сталкиваются с шифрами. В этих рассказах для дешифровки был использован частотный криптоанализ, который был изобретен в IX веке и описан в «Манускрипте о дешифровке криптографических сообщений» арабским учёным Ал-Кинди[1].

Мне нравится самому придумывать новые шифры, но для этого нужно сначала изучить и понять алгоритмы работы шифров, изобретенных до меня. Поэтому я и решил изучить наиболее известные шифры древности и их возможности.

Частотный криптоанализ помогает людям уже больше тысячи лет, и даже сейчас при помощи этого способа дешифровки возможно взломать большинство существующих шифров.

Возможности применения криптографии очень широки:

- Война. Секретная передача данных о планах и перемещениях войск, их составе и численности.
- Политика. Борьба политических партий, вопросы внешней политики.
- Наука. Тайны научных открытий, рецептур, тайное общение представителей одной научной школы.
- Религия. Шифрование священных текстов для обеспечения секретности и придания таинственности.
- Личная жизнь. Тайные любовные послания, завещания, детские игры.

[1] Википедия, http://ru.wikipedia.org/wiki/Криптоанализ

Цель, задачи работы

Цель данной работы:

- рассмотреть возможности некоторых, самых известных и интересных шифров древности

Задачи работы:

- познакомиться с историей криптографии,
- создать модели некоторых шифров древности,
- проверить на практике механизм их использования для передачи сообщений, а также возможность взлома.

Методы

Чтобы оценить возможности шифров, мы создадим их действующие модели из подручных средств (картон, шнур, деревянные цилиндры) и на практике оценим сложность процесса зашифровки, дешифровки и взлома шифров.

Актуальность темы

Эта тема особенно актуальна в наше время, поскольку «информация становится все более ценным товаром, а революция в сфере коммуникаций изменяет общество».[2] Шифрование становится единственным способом защитить частную жизнь человека.

Источники и литература

Большинство авторов книг и научно-исследовательских работ по криптографии уделяют внимание более сложным и современным шифрам и кодам, а древняя криптография остаётся в тени. Полноценные главы о древних методах шифрования я встретил в книге Риксона Фреда Б. «Коды, шифры, сигналы и тайная передача информации», а также книге Сингха Саймона «Книга шифров: тайная история шифров и их расшифровки».

[2] Сингх, Саймон. Книга шифров: тайная история шифров и их расшифровки, М: АСТ, 2007, с. 10

Глава 1 Теоретические основы криптографии

Перед тем как рассматривать шифры, необходимо договориться о терминах, которые составляют основу криптографии.

Криптография – методы сокрытия содержания сообщения с помощью кодов или шифров.

Криптоанализ (взлом) – процесс извлечения открытого текста из зашифрованного сообщения без знания ключа.

Шифр – способ сокрытия информации, в котором основным элементом является буква. Буквы открытого текста заменяются на другие буквы, числа или символы, буквенные пары, а иногда более крупные группы

Код – способ сокрытия информации с использованием слов, чисел или слогов, для замены исходных слов или фраз сообщения. При применении кодов заменяются целые слова, в то время как в кодах заменяются буквы или пары букв.

Шифртекст (закрытый текст) – результат применения шифрметода к тексту. Зашифрованный текст является шифртекстом.

Открытый (исходный) текст – сообщение, передаваемое без зашифровывания или кодирования, а также сообщение до того, как его зашифруют или после того, как его расшифруют.

Ключ – инструкции, которые управляют ходом зашифровывания (кодирования) и расшифровывания (раскодирования) сообщений.

Шифрование – процесс преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.

Дешифровка – удаление шифра, скрывающего содержание сообщения. Выполняется адресатом, имеющим верный ключ.

Глава 2 История криптографии

Периоды развития криптографии

Криптография появилась около четырех тысяч лет назад. За это время ее история прошла несколько периодов, на протяжении которых использовались разные методы шифрования. В Википедии описываются следующие пять периодов:

Первый период (приблизительно с 3-го тысячелетия до н. э.) характеризуется господством моноалфавитных шифров (основной принцип – замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами).

В древности подавляющее большинство людей были неграмотными, поэтому основные способы шифрования были достаточно простыми. Но уже в античные времена существовало множество разнообразных шифров основанных на различных методах шифрования.

В рамках данной работы мы разберем некоторые шифры первого периода развития криптографии.

Второй период (с IX века на Ближнем Востоке (Ал-Кинди) и с XV века в Европе (Леон Баттиста Альберти) – до начала XX века) ознаменовался введением в обиход полиалфавитных шифров.

Третий период (с начала и до середины XX века) характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.

Четвёртый период – с середины до 70-х годов XX века – период перехода к математической криптографии. Однако до 1975 года криптография оставалась «классической» (с секретным ключом).

Современный период развития криптографии (с конца 1970-х годов по настоящее время) отличается зарождением и развитием нового направления – криптография с открытым ключом. Её появление знаменуется не только новыми техническими возможностями, но и сравнительно широким распространением криптографии для использования частными лицами.[3]

[3] Википедия (http://ru.wikipedia.org/wiki/История криптографии)

Шифры Древнего Мира

Скитала

Доподлинно неизвестно, когда появился шифр перестановки, но один из самых ранних известных примеров – это скитала. Скорее всего, впервые скитала упоминается греческим поэтом Архилохом, жившим в VII веке до н. э.

Скитала – первое известное шифровальное устройство, которое представляло собой деревянный цилиндр или жезл. На этот цилиндр наматывалась полоска кожи, на которой писали исходный текст (Приложение, рис.1). После снятия ленты со скитали текст становился беспорядочной последовательностью букв (Приложение, рис.2). Если намотать ленту на скиталу другого диаметра, текст также не читается (Приложение, рис.3).

В 404 году до н.э., к спартанскому полководцу Лисандру привели вестника, окровавленного и еле держащегося на ногах, одного из пяти оставшихся в живых после крайне опасного путешествия из Персии. Вестник передал свой пояс Лисандру, который намотал его вокруг своей скитали и прочитал, что Фарнабаз (персидский сатрап и военачальник) собирается напасть на него. Благодаря скитале Лисандр успел подготовиться к нападению и отбил его.[4]

Свидетельствует об использовании скитали и историк Плутарх:

> *А скитала вот что такое. Отправляя к месту службы начальника флота или сухопутного войска, эфоры*[5] *берут две круглые палки совершенно одинаковой длины и толщины. Одну они оставляют себе, другую передают отъезжающему. Эти палки и называют скиталами. Когда эфорам нужно сообщить какую-нибудь важную тайну, они вырезают длинную и узкую, вроде ремня, полосу папируса, наматывают её на свою скиталу, не оставляя на ней ни одного промежутка, так чтобы вся поверхность палки была охвачена этой полосой. Затем, оставляя папирус на скитале в том виде, как он есть, они пишут на нем то, что нужно, а написав, снимают полосу и без палки отправляют ее военачальнику. Так как буквы на ней стоят без всякой связи, но разбросаны в беспорядке, прочитать написанное он может, только взяв свою скиталу и намотав на нее вырезанную полосу, располагая ее извивы в прежнем порядке, чтобы, водя глазами вокруг палки и переходя от предыдущего к последующему, иметь перед собой связное сообщение. Полоса папируса называется, как и деревянная палка, «скиталой», подобно тому как измеряемый предмет называется по мере.*
> – Плутарх, *Сравнительные жизнеописания* (Лисандр), пер. М. Е. Сергеенко.

Как понятно из этого текста, дешифровка происходила при наматывании ленты на идентичную скиталу.

При зашифровке при помощи скитали открытого текста

[4] Сингх, Саймон, Книга шифров: тайная история шифров и их расшифровки, с.23
[5] В Древней Спарте – выборные должностные лица.

криптография в древнем мире

будет

КТАВВМРОФДНИИГИРЕПРПЯЕМЕ

Первым, кто сумел взломать скиталу, считается Аристотель, который предложил наматывать ленту на конус в разных местах, пока не появлялись куски осмысленного текста. Так выяснялся диаметр скиталы.

Но можно взломать шифр скиталы еще проще, путем подбора: любые две буквы, которые в исходном тексте находились на соседних местах, в шифровке будут располагаться на одном расстоянии друг от друга. Зная это, можно подобрать размер этого сдвига.[6]

В нашей модели скиталы этот сдвиг равен 6.

Эней

В IV в.до н.э. Эней Тактик, греческий политический деятель и полководец, а также автор трудов об искусстве войны, изобрел способ передачи информации при помощи диска.

Диск Энея представлял собой деревянный диск с просверленными вдоль края дырками по количеству букв алфавита, и двумя отверстиями в центре. Буквы шли по порядку, и поэтому обозначалась только первая буква: на нее указывало расположение двух центральных отверстий (Приложение, рис.4). В отверстия вставлялась нить в соответствии с исходным текстом. Чтобы зашифровать повторяющиеся буквы использовались отверстия в середине диска. Вначале нить продевалась в него, а затем в повторяющийся символ (Приложение, рис.5).

Сообщение посылалось с диском, и прочесть его мог любой, кто смог завладеть диском. Но Эней придумал способ быстро уничтожить сообщение. Для этого достаточно было сломать диск, наступив на него ногой. После этого текст невозможно было прочитать, так как диск обычно ломался в местах просверленных отверстий, в результате чего нить спутывалась.

Получатель должен был, постепенно вытаскивая нить, выписывать буквы, при этом он получал текст наоборот. Например, после дешифровки при помощи диска Энея открытый текст

криптография в древнем мире

будет

ЕРИМ МЕНВЕРД В ЯИФАРГОТПИРК

На самом деле диск Энея нельзя назвать настоящим криптографическим инструментом, поскольку прочитать сообщение мог любой желающий.

[6] Математический Клуб Кенгуру, выпуск 14 «Шифры и математика», с.4

Но это изобретение получило развитие, идея которого тоже принадлежит Энею – это так называемая линейка Энея, которая представляет собой небольшую палочку с отверстиями по количеству букв алфавита, буквы по отверстиям располагались в произвольном порядке. При шифровании послания нитка продевалась через отверстия, каждый раз проходя через отверстие в начале линейки. В местах, где нить продевалась через отверстия, завязывались узелки. В отличие от диска, нитка посылалась без линейки, что обеспечивало лучшую защиту от взлома, поскольку прочитать сообщение можно было, только имея идентичную линейку.

Такой шифр является одним из примеров шифра замены: когда буквы заменяются на расстояния между узелками с учетом прохождения через прорезь.

Ключом шифра являлся порядок расположения букв по отверстиям в линейке. Посторонний, получивший нить (даже имея линейку, но без нанесенных на ней букв), не сможет прочитать передаваемое сообщение.

Кроме того, Эней изобрел так называемый «книжный шифр»: над буквами определенной книги прокалывались маленькие дырочки. Выписав последовательно все помеченные буквы, адресат мог понять смысл послания. Данный метод относится не к шифрам, а к стеганографии, или тайнописи.

Квадрат Полибия

Греческий историй и криптограф Полибий, живший во II веке до н.э., изобрел интересный шифр, представляющий собой таблицу со вписанными в нее буквами алфавита. Квадрат Полибия является шифром замены.

У каждой буквы присутствует горизонтальная и вертикальная координата, обозначенная цифрой, их сочетание и обозначает зашифрованную букву (Приложение, рис.6). При шифровании буква заменялась своими координатами и представляла собой двузначное число. Для дополнительной защиты, при заполнении квадрата буквами алфавита можно было сначала писать ключевую фразу, не используя потом те же буквы повторно.

При зашифровке при помощи квадрата Полибия фраза

криптография в древнем мире

будет

26 36 24 35 42 14 36 11 44 24 63 13 15 36 16 13 33 16 32 32 24 36 16

Послание можно было дешифровать, находя по координатам, вертикальной и горизонтальной, букву текста. Буква за буквой, сообщение дешифровалось.

Этот шифр можно взломать при помощи частотного анализа, но рассматривать надо блоки из двух цифр.

Некоторые исследователи полагают, что квадрат Полибия можно рассматривать как первую систему, уменьшавшую (сжимавшую) исходный алфавит, и как прообраз современной системы двоичной передачи данных.[7]

На основе квадрата Полибия в более позднее время был придуман «тюремный шифр», в котором цифровые координаты буквы выстукивались на стене тюремной камеры, а также шифр Элизабет Ван Лью времен Гражданской Войны в Америке.[8]

Шифр Цезаря

Гай Юлий Цезарь (12 или 13 июля 102 года до н.э.; по другим данным – 100 год до н.э – 15 марта 44 года до н.э.) – великий древнеримский политик и государственный деятель, диктатор, полководец и писатель, изобрел для передачи сообщений простой, но широко известный метод шифрования, впоследствии названный его именем.

> *Если у него было что-либо конфиденциальное для передачи, то он записывал это шифром, то есть так изменял порядок букв алфавита, что нельзя было разобрать ни одно слово. Если кто-либо хотел дешифровать его и понять его значение, то он должен был подставлять четвертую букву алфавита, а именно, D, для A, и так далее, с другими буквами.*
> - Гай Светоний Транквилл, *Жизнь двенадцати цезарей 56.*

Как видно из этой цитаты, шифр Цезаря – это вид шифра простой замены, в котором каждый символ в открытом тексте заменяется буквой, находящейся на некоторое постоянное число позиций левее или правее него в алфавите. Например, в шифре со сдвигом на 3, буква А была бы заменена на Г, Б станет Д, и так далее.

Есть и другие варианты этого шифра, с меньшим или большим сдвигом в шифралфавите. То есть А-Е, Б-Ё, В-Ж (для сдвига на 5).

Для более быстрой и удобной зашифровки и дешифровки можно было использовать диск, который состоял из 2 кругов разного размера на одной оси, с написанными по окружности буквами алфавита. На внешнем диске располагался открытый алфавит, а на внутреннем – шифралфавит. Для зашифровывания и расшифровывания требовалось повернуть диск на несколько букв. Сопоставляя буквы, получаем зашифрованный текст (Приложение, рис.7).

Например, после зашифровки при помощи шифра Цезаря со сдвигом на 4 буквы

криптография в древнем мире

будет

НУЛТХСЖУГЧЛВ Е ЗУИЕРИП ПЛУИ

[7] Википедия (http://ru.wikipedia.org/wiki/История_криптографии)
[8] Риксон, Фред Б. Коды, шифры, сигналы и тайная передача информации. М: АСТ, 2011,с.178

Шифр Цезаря может быть легко взломан даже в случае, когда взломщик знает только зашифрованный текст. Цезарю повезло, так как большинство его врагов были неграмотны или полагали, что это неизвестный язык!

При взломе возможны 2 варианта:

1. взломщик знает (или предполагает), что использовался простой шифр замены, но не знает, что это – шифр Цезаря;
2. взломщик знает, что использовался шифр Цезаря, но не знает значение сдвига.

В первом случае шифр может быть взломан, используя те же самые методы, что и для простого шифра замены, такие как частотный анализ. Используя эти методы, взломщик, вероятно, быстро заметит регулярность в решении и поймёт, что используемый шифр – это шифр Цезаря.

Во втором случае, взлом шифра является даже более простым. Существует не так много вариантов значений сдвига (26 для английского языка и 33 для русского), все они могут быть проверены методом грубой силы. Один из способов сделать это – выписать отрывок зашифрованного текста в столбец всех возможных сдвигов – техника, иногда называемая как «завершение простого компонента»[9]. Рассмотрим пример для зашифрованного текста «***НУЛТХСЖУГЧЛВ***»; открытый текст быстро опознается в третьей строке.

1 мткcфретвцкб

2 лсйрупдсбхйа

3 криптография

4 йпзоснвпяузю

…..

[9] Википедия (http://ru.wikipedia.org/wiki/Шифр Цезаря)

Заключение

Рассмотрев основные шифры древности, изучив их описания в общедоступных источниках и создав на их основе действующие модели шифровальных устройств, мы создали сравнительную таблицу шифров древности. Мы расставили им оценки по определённым критериям (данные в таблице, Приложение №2) и пришли к следующим выводам:

1. Шифры древности достаточно просты в применении. Без специального оборудования мы смогли изготовить из подручных средств работающие модели шифровальных устройств, и воспроизвели процедуры шифровки и расшифровки.
2. Шифры древности достаточно просто взламываются. Используя несложные приемы, мы смогли воспроизвести процедуры взлома.

Изучая шифры древности, мы видим некоторые приёмы, которые присущи сразу нескольким шифрам. Общим для рассмотренных шифров является то, что вся информация шифруется «в один шаг».

Идея замены символов исходного текста также присутствует в нескольких шифрах. Алгоритмы, по которым происходят замены в шифрах первого периода развития криптографии, просты.

Таким образом, мы видим, что возможности криптографии Древнего Мира были существенно ограничены, в связи со слабым развитием письменности и математики. Вообще, криптография всегда была тесно связана с математикой, хотя была признана математической наукой совсем недавно, в конце XX века.

Материалы этой работы могут быть использованы на уроках истории древнего мира при изучении Древней Греции и Древнего Рима, для лучшего усвоения и закрепления темы.

В следующей работе мы сможем проследить развитие математических алгоритмов шифрования и дешифровки в более поздние периоды.

Литература

1. Математический Клуб Кенгуру, выпуск 14 «Шифры и математика»

2. Риксон, Фред Б. Коды, шифры, сигналы и тайная передача информации. М: АСТ, 2011

3. Сингх, Саймон, Книга шифров: тайная история шифров и их расшифровки, М: АСТ, 2007

4. Википедия http://ru.wikipedia.org/

Приложение 1. Иллюстрации.

Рис. 1. Скитала с намотанной лентой.

Рис. 2. Лента, снятая со скиталы.

Рис. 3. Нечитаемый текст на скитале другого диаметра.

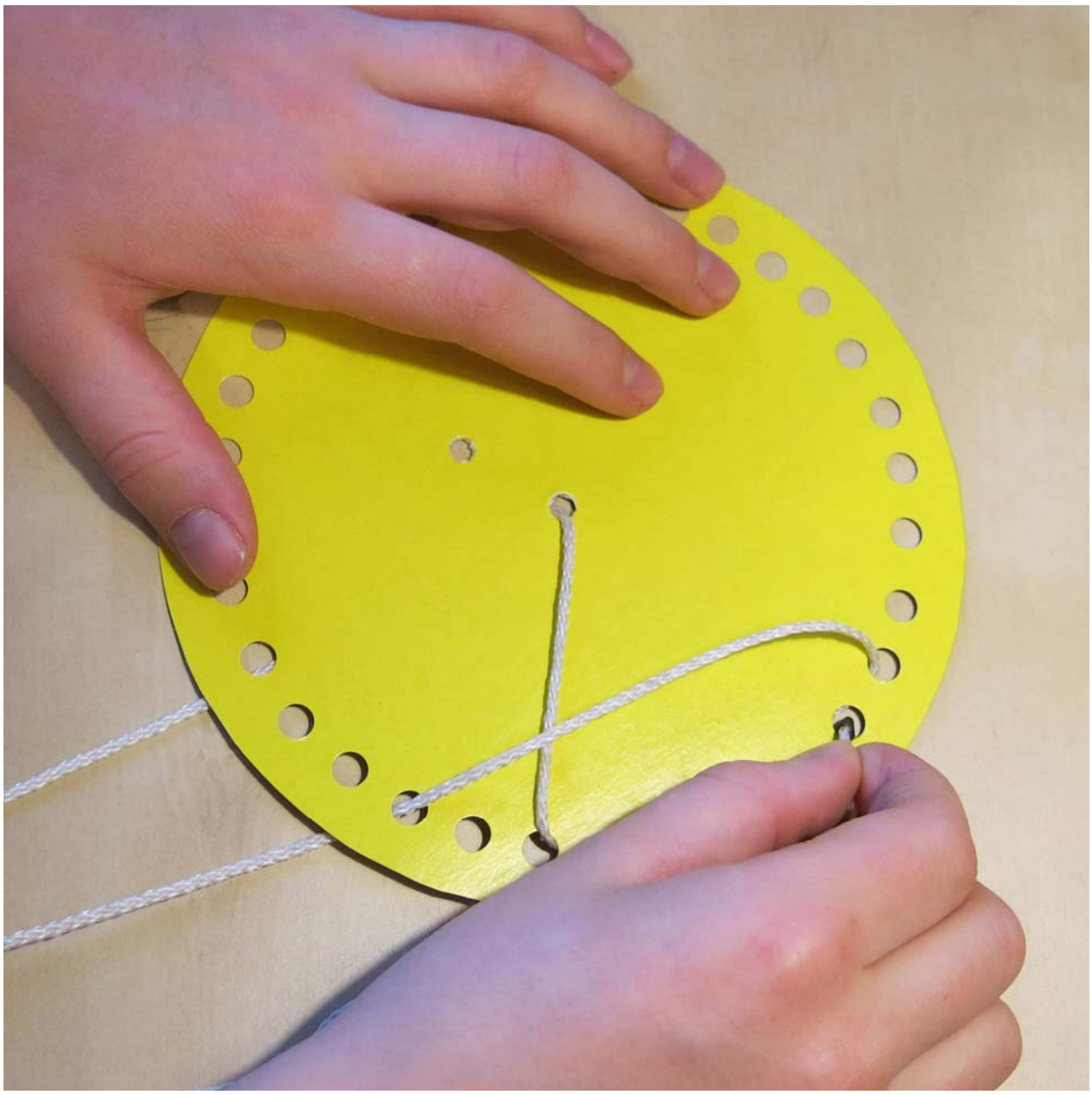

Рис. 4. Диск Энея – процесс зашифровки.

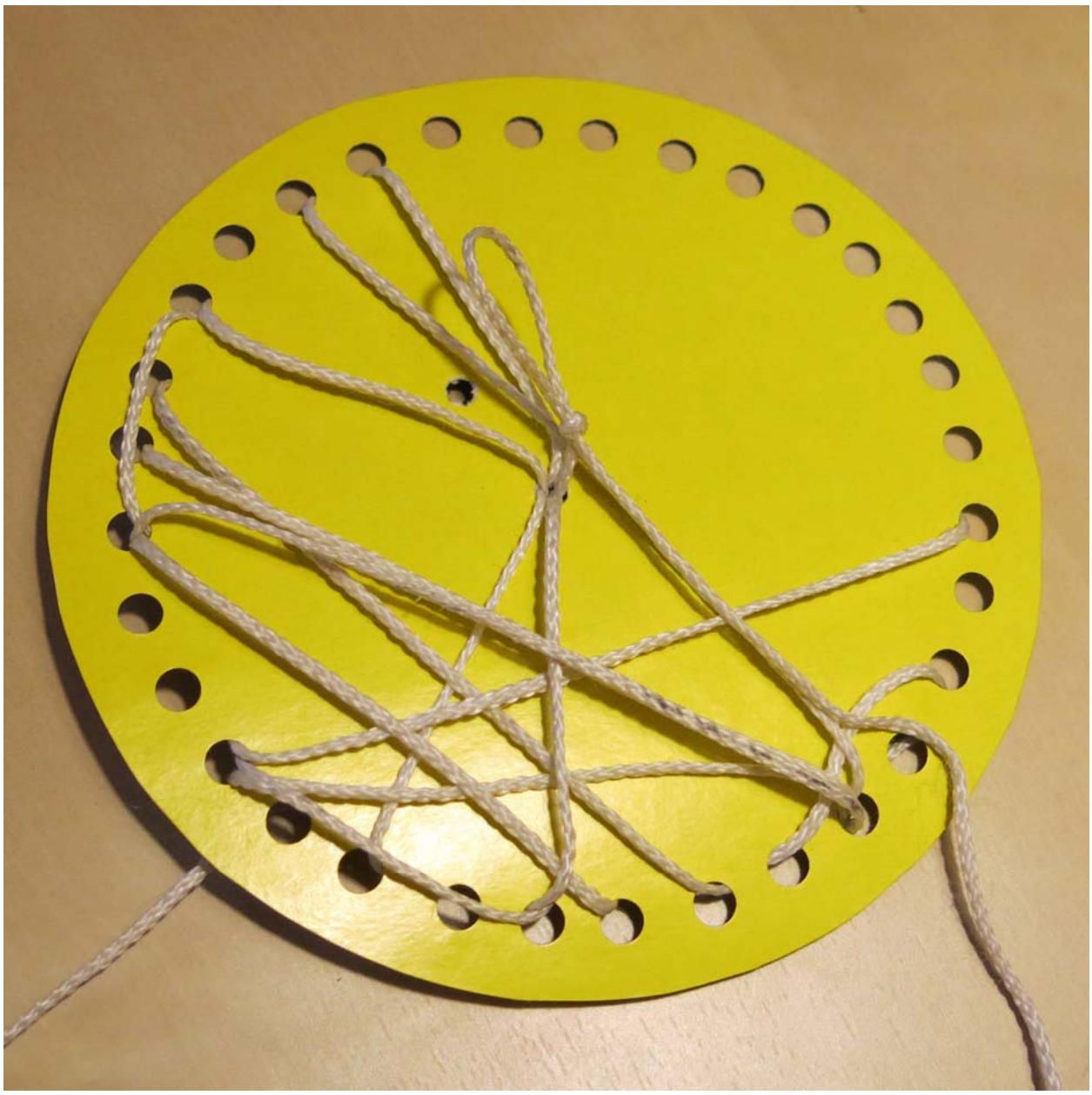

Рис. 5. Диск Энея с шифртекстом.

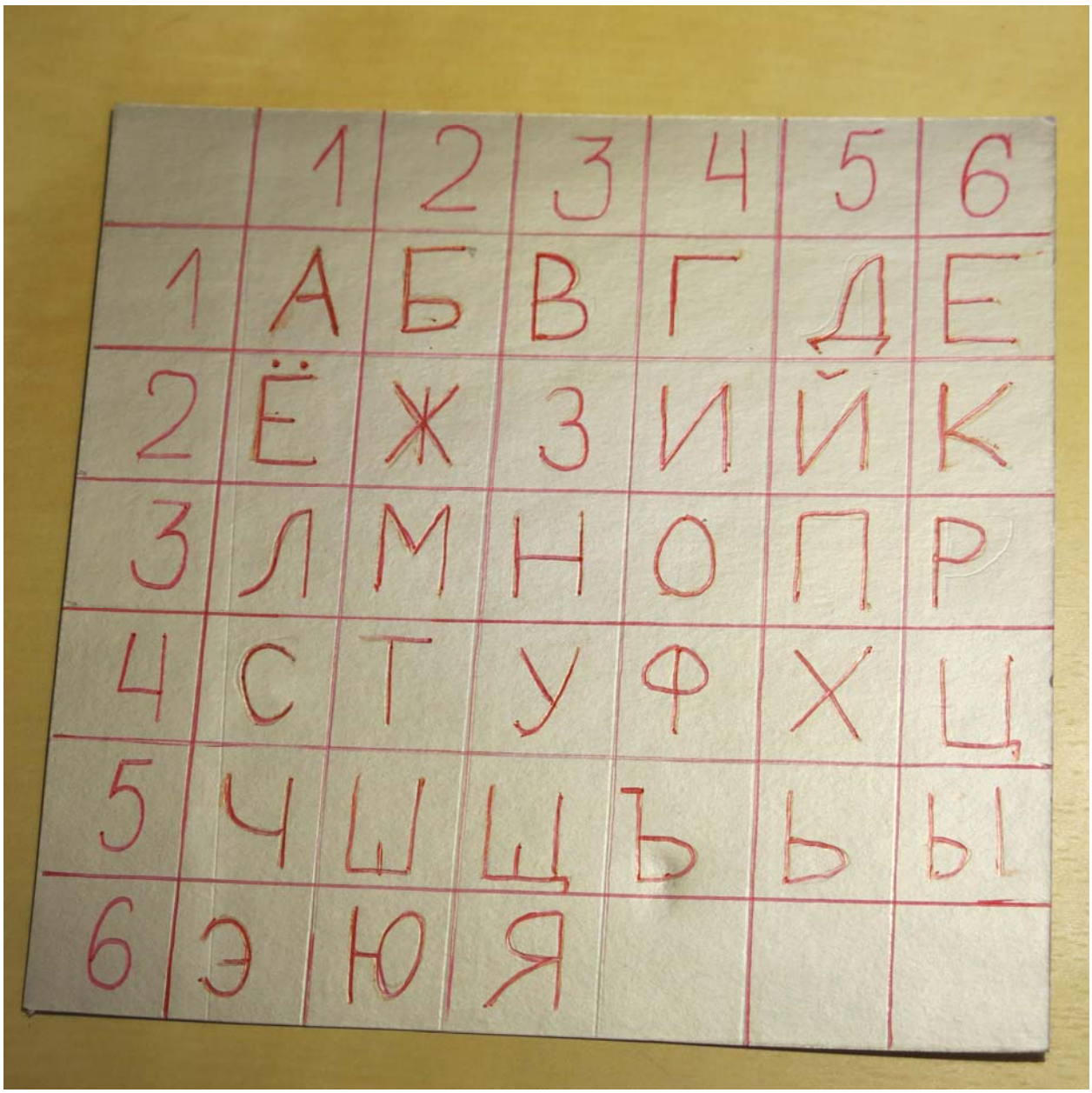

Рис. 6. Квадрат Полибия 6x6 для русского алфавита.

Рис. 7. Шифр Цезаря. Диск для шифрования.

Приложение 2. Сравнительная таблица шифров древности

	Тип шифра	Время возникновения	Место возникновения	Сложность зашифровки	Сложность расшифровки	Сложность взлома	Примечания
				место	место	место	
Скитала	Шифр перестановки	VII в.до н.э.	Спарта (Древняя Греция)	4	3	2	Непросто пользоваться для зашифровки и расшифровки сообщений, при этом взломать ее просто, т.к. буквы не заменяются, нужно просто найти правильный порядок
Диск Энея	Стеганография	IV в. до н.э.	Стимфал (Древняя Греция)	3	4	1	Шифровать и расшифровывать несложно, но манипуляции с нитью отнимают много времени. Если диск поврежден, дешифровка невозможна
Квадрат Полибия	Шифр замены	II в. до н.э.	Аркадия (Древняя Греция)	1	1	4	Просто шифровать и дешифровать, взлом, если буквы расположены в хаотичном порядке – только с применением частотного анализа.
Шифр Цезаря	Шифр замены	I в. до н.э.	Древний Рим	2	2	3	Просто шифровать и дешифровать, взломать можно методом грубой силы (техника «завершение простого компонента»)