BIT BOOK

ПРО КРИПТОГРАФИЮ

WWW.SYMBOL-SIGN.COM

У КНИГИ ЕСТЬ САЙТ

ПРОСТО

УДК 001, 501, 510
ББК 22.1
К 28

К 28 ПРО КРИПТОГРАФИЮ (Символ — машина — квант) — СПб.: Страта, 2020. — 240 с., с илл. — (серия «Просто»)

ISBN 978-5-907314-15-3

Чем больше одни стремятся что-то скрыть, тем больше другие хотят это «что-то» узнать. Когда люди только научились писать, их тайны материализовались, представ в образе символов, иероглифов, букв, цифр. Но в таком виде они стали доступны другим. С этого времени началось извечное соревнование между шифровальщиками, пытающимися скрыть информацию, и криптоаналитиками, стремящимися расшифровать ее.

Криптография сегодня — это область научных, прикладных, инженерно-технических исследований, основанная на фундаментальных понятиях математики, физики, теории информации и сложности вычислений.

В книге рассказывается об истории криптографии: от примитивных систем шифрования и дешифровки, придуманных людьми еще в древние времена, до современных компьютерных алгоритмов — как существующих, так и тех, над которыми работают нынешние ученые-криптографы.

Книга предназначена для широкого круга читателей.

УДК 001, 501, 510
ББК 22.1

ISBN 978-5-907314-15-3

СОДЕРЖАНИЕ

ГЛАВА I.
КОДИРОВАНИЕ И ШИФРОВАНИЕ

«На свете множество неразгаданных шифров, непонятых языков, загадочных тайнописей и нерасшифрованных карт… Карты, языки, коды, шифры разгадываются и декодируются каждый день, порой этому предшествуют мучительные годы исследований и расчетов. Последние разработки позволяют расшифровывать ранее непонятные и неразборчивые языки при помощи компьютера».

Livejournal.com

ОТ ОСКОЛКА — К КУБИТУ

Искусство создания посланий, которые могут быть поняты только отправителем и получателем, а любому другому покажутся абсолютно бессмысленными, известно давно. В Древней Греции разбивали горшок и два соседних осколка передавали незнакомым людям, чтобы они, встретившись, могли распознать друг друга, чтобы отличать своих от чужих.

Историки знают о существовании ряда «нестандартных» иероглифов, которым более четырех с половиной тысяч лет. Хотя, конечно, вряд ли возможно с полной уверенностью сказать, представляют ли они попытку скрыть информацию или просто использовались в некоем религиозном ритуале... Зато хорошо известно о табличке из Вавилона, датированной примерно 2500 годом до н. э. На ней есть слова, в которых удален первый согласный и использован целый ряд необычных вариантов обозначения звуков. Исследования показали, что в тексте описан способ изготовления глазури для гончарных изделий, а это приводит нас к выводу: текст был написан купцом или мастером-гончаром, пожелавшим защитить от конкурентов секреты своего мастерства.

По мере распространения письменности и торговли возникли великие империи, которые часто вступали в пограничные конфликты со своими географическими соседями. В результате криптография и безопасная передача информации стали делом особой важности не только для купцов, но и для правительств.

Схема шифрования в самом общем виде определялась следующими элементами: отправитель послания, получатель послания, алгоритм шифрования и определенный ключ, который позволяет отправителю шифровать послание, а получателю

расшифровывать его. Природа и функция ключей изменилась, но пока будем придерживаться этой схемы.

Изначальная цель кодирования — техническое обеспечение связи. Например, текст конвертируется в бинарный (или двоичный) язык (систему счисления, использующую только цифры 0 и 1). После кодирования большая часть этой информации должна быть защищена от любого, кто может ее перехватить. Другими словами, кодированное послание требуется зашифровать. Наконец, законный получатель должен быть способен расшифровать полученное послание.

Кодирование, шифрование и дешифровка — это основные па в «танце информации», который повторяется миллионы раз в секунду, каждую минуту, каждый час каждого дня.

А «музыка», сопровождающая этот танец, — математика.

КОД И ШИФР

Шифровальщики и специалисты по криптографии используют термин «кодировать» в несколько ином смысле. Для них кодирование — это метод написания с использованием кода, который состоит из замены одного слова другим. С другой стороны, использование шифра, или шифрование, включает замену букв или каких-то других отдельных знаков. С течением времени в широком сознании последняя форма сделалась превалирующей, причем в такой степени, что стала синонимом «написания с использованием кода», или «закодированного письма». Однако если мы возьмем более строгое научное определение, то для второго метода правильным термином будет «шифровать» (или «расшифровывать», в случае обратного процесса) послание.

Давайте представим, что мы отправляем защищённое послание «АТАКОВАТЬ». Мы можем сделать это двумя основными путями: заменить слово целиком (кодирование), заменить некоторые или все буквы, которые составляют это слово (шифрование). Простой способ кодирования слова — перевести его на язык, который не знают потенциальные любители подслушать или подсмотреть. В случае шифрования будет достаточно, например, заменить каждую букву другой (то есть стоящей в другой части алфавита). В этом случае необходимо, чтобы получатель знал использовавшуюся процедуру для того, чтобы декодировать или дешифровать текст, или послание потеряет смысл. Если мы уже договорились с получателем, что будем использовать тот или иной способ — переводить на другой язык или заменять каждую букву, — то всё, что от нас

Табличка, найденная на Крите, на которой используется так называемое «линейное письмо Б»

требуется, — это сообщить нашему получателю о выбранном языке или количестве позиций, на которые мы продвинулись в алфавите для замены каждой буквы.

В приводимом примере, если получатель получает зашифрованное послание «ВФВЙРДВФЮ» и знает, что при замене каждой буквы мы сдвигались на две позиции вперёд в алфавите русского языка, то он сможет с лёгкостью повторить процесс, двигаясь в обратном направлении, и успешно расшифровать послание.

Установленное нами разграничение между правилом шифрования (применяемая система) и параметром шифрования [меняющееся указание (инструкция), которое является специфическим для каждого послания или набора посланий] очень полезно, потому что потенциальному шпиону для расшифровки нужно знать и то, и другое.

Таким образом, шпион может знать, что ключ к шифру — это замена каждой буквы другой, находящейся далее в алфавите через определённое количество позиций (x). Однако если он не знает, какому числу соответствует x, то ему потребуется перепробовать все возможные комбинации для каждой буквы алфавита. В этом примере шифр очень простой, и испробовать все возможности — для чего требуется просто усердие — не так уж и сложно.

Эта техника дешифровки называется *методом тотального перебора*. Однако в более сложных случаях такой тип взлома кода (криптоанализ) практически невозможен — по крайней мере, вручную. Более того, на перехват и расшифровку посланий обычно накладываются жёсткие временные ограничения. Ведь информацию нужно получить и понять прежде, чем она станет бесполезной или широко известной другим.

Общее правило шифрования обычно называется *алгоритмом шифрования*, в то время как специфический параметр, используемый для шифрования или кодирования послания, называется *ключом* (в примере шифрования, приведённом выше, ключ — 2. Каждая буква исходного слова заменяется другой, которая расположена через две позиции в алфавите русского языка).

СКОЛЬКО НУЖНО КЛЮЧЕЙ?

Какое минимальное количество ключей необходимо в системе с двумя пользователями? Тремя? Четырьмя? Чтобы два пользователя могли тайно общаться друг с другом, необходим только один ключ. В случае трёх пользователей (A, B и C) необходимы три ключа: один для общения A и B, ещё один для пары A и C, а третий — для пары B и C. Точно так же четырём пользователям потребуется шесть ключей. Таким образом, если обобщить, то для *n* пользователей потребуется столько ключей, сколько существует комбинаций пар из *n*, то есть:

$$\frac{n}{2} = \frac{n(n-1)}{2}$$

В результате для относительно небольшой системы из 10000 связанных между собой пользователей потребуется 49 995 000 ключей. Если взять население земного шара, составляющее шесть миллиардов человек, то от количества ключей голова пойдёт кругом:

17 999 999 997 000 000 000.

Очевидно, что для каждого алгоритма шифрования возможно огромное количество ключей, поэтому знание одного алгоритма может быть бесполезным, если мы не имеем представления, какой ключ нужен для расшифровки. Поскольку ключи обычно легче заменить и распространить, кажется логичным для обеспечения безопасности системы шифрования сосредоточиться на том, чтобы хранить ключи в тайне и уделять именно этому максимальное внимание. Такой принцип был установлен в конце XIX столетия голландским лингвистом Огюстом Керкгоффсом фон Ниевенхофом и поэтому известен как принцип Керкгоффса.

ПРИНЦИП КЕРКГОФФСА

В соответствии с принципом Керкгоффса, ключ — это основной элемент, обеспечивающий безопасность криптографической системы. До относительно недавнего времени ключи отправителя и получателя во всех возможных криптографических системах должны были быть идентичными или по крайней мере симметричными, то есть их необходимо было использовать и для шифрования, и для расшифровки послания. Поэтому ключ являлся общей тайной отправителя и получателя, и, таким образом, используемая криптографическая система была уязвимой с обеих сторон. Этот тип криптографии, который зависит от ключа, имеющегося как у отправителя, так и у получателя, называется «шифрование закрытым ключом».

Это было свойством всех криптографических систем, изобретённых людьми с начала времён, независимо от используемого алгоритма и сложности. Сделать ключ одним и тем же для получателя и отправителя кажется единственно разумным и полностью соответствующим здравому смыслу.

Как мы видели выше, для классической криптографии требовалось огромное количество ключей. Однако в случае открытой (общедоступной) криптографической системы любым двум пользователям, которые обмениваются посланиями, требуются только четыре ключа: их соответствующие открытые и закрытые ключи. В этом случае количеству пользователей n требуется $2n$ ключей.

В конце концов, разве может один человек кодировать послание в соответствии с одним кодом, а второй расшифровывать его в соответствии с другим и надеяться понять полученный текст? Тысячи лет это считалось полным абсурдом. Однако, как мы увидим ниже, всего пять десятилетий назад абсурд стал абсолютно возможным и теперь используется повсеместно.

В наши дни алгоритмы шифрования, которые используются в большинстве коммуникационных связей, состоят, как правило, из двух ключей: закрытого ключа, который уже

Доктор Огюст Керкгоффс

стал обычным делом, и открытого ключа, который знают все. Механизм передачи состоит в следующем: отправитель получает открытый ключ получателя, которому хочет отправить послание, и использует его для шифровки послания. Получатель использует свой закрытый ключ для расшифровки полученного послания.

Более того, эта система имеет очень важное дополнительное преимущество: ни отправителю, ни получателю не нужно заранее встречаться и договариваться ни о каких используемых ключах, поэтому безопасность системы гораздо выше, чем было возможно ранее.

Эта полностью революционная форма известна как «шифрование открытым ключом» и сегодня составляет основу безопасности в коммуникационных сетях. Фактически, как мы подробно выясним ниже, современная криптография держится на двух китах. Первый — модульная арифметика, а второй — теория чисел и в особенности та ее часть, которая занимается изучением простых чисел.

ТЕЛЕГРАММА ГЕРМАНСКОМУ ПОСЛУ

Криптография — это одна из областей прикладной математики, в которой наиболее очевиден контраст между первоначальной четкостью, лежащей в основе теории, и туманными последствиями ее внедрения и применения на практике.

А ведь иногда от успеха или провала в обеспечении защиты связи и коммуникаций зависит судьба целых наций. Одним из самых впечатляющих примеров того, как криптография изменила курс истории почти сто лет назад, является так называемое «дело о телеграмме Циммермана».

7 мая 1915 года, когда половина Европы была вовлечена в кровавый конфликт Первой мировой войны, немецкая подводная лодка торпедировала трансатлантический пассажирский лайнер «Лузитания», шедший под британским флагом недалеко от берегов Ирландии. Результатом стала одна из наиболее ужасных трагедий в истории: погибли 1198 гражданских лиц, 124 из которых были американцами.

Новость вызвала ярость в общественном мнении Соединенных Штатов Америки, и администрация президента Вудро Вильсона предупредила немецкое правительство, что если подобное повторится, США немедленно вступят в войну на стороне союзников. В дополнение к этому Вильсон потребовал, чтобы немецкие подводные лодки придерживались правил ведения морской войны, установленных Гаагскими конвенциями 1899 и 1907 годов, что ставило под угрозу преимущество немецкого флота, применяющего по отношению к гражданским судам тактику неограниченной подводной войны.

В ноябре 1916 года Германия назначила новым министром иностранных дел Артура Циммермана, имевшего репутацию прекрасного дипломата. Новость была положительно принята прессой США, которая посчитала это назначение благоприятным знаком для американо-германских отношений.

В январе 1917 года, менее чем через два года после трагедии с «Лузитанией», когда война была в самом разгаре, посол Германии в Вашингтоне Иоганн фон Бернсторф получил от Циммермана следующую зашифрованную телеграмму с указанием тайно передать ее коллеге, германскому послу в Мексике, Генриху фон Эккардту:

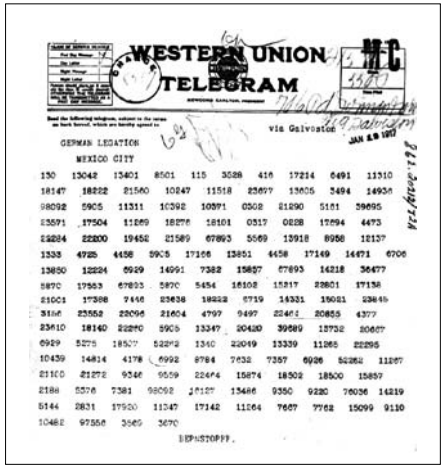
«Мы намерены с первого февраля возобновить неограниченную подводную войну. Тем не менее, следует предпринять все попытки к тому, чтобы США и дальше сохраняли нейтралитет. Однако, если такие попытки окажутся безуспешными, мы предложим Мексике заключить союз на следующих условиях: совместное ведение боевых действий и совместное заключение мира; серьезная финансовая поддержка с нашей стороны и понимание нами стремления Мексики по возвращению утраченных территорий в Техасе, Нью-Мексико и Аризоне. Детали соглашения оставляются на ваше усмотрение [фон Эккардта].

Вы должны довести до сведения Президента [Мексики] о вышеуказанном с соблюдением максимальной степени секретности, как только станет точно известно о начале войны с США, и в дополнение к этому предложить ему по собственной инициативе пригласить Японию для немедленного присоединения к союзу и стать посредником между Японией и нами.

Пожалуйста, обратите внимание Президента на тот факт, что использование наших подводных лодок в полной мере открывает перспективу заставить Англию в течение нескольких месяцев заключить мир».

Если бы содержание телеграммы сделалось достоянием общественности, это наверняка бы привело к началу войны между Германией и США.

Кайзер Вильгельм II, разумеется, понимал, что после того как немецкие подводные лодки начнут действовать с нарушением Гаагских конвенций, война сделается неизбежной, однако он надеялся, что к тому времени Великобритания капитулирует, и США попросту не успеют включиться в завершившийся военный конфликт. К тому же активная угроза со стороны Мексики у южных рубежей США заставит американцев сто раз подумать, прежде чем вступать в конфликт, происходящий вдали от их границ.



WESTERN UNION
TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3028 416 17214 6491 11310
18147 18822 21560 10247 11518 25677 13605 3494 14936
98092 5905 11311 10392 10971 0502 21290 5161 39695
13571 17504 11269 18076 18101 0317 0828 17694 4473
12284 22800 19452 21389 67893 5569 13918 8958 12137
1338 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17563 67893 5870 5454 16108 15217 22801 17138
21001 17388 9446 23638 18822 6719 14331 15081 23845
3156 25552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22290 5905 13347 20420 39589 18732 20667
6929 5275 18507 52292 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2184 5376 7381 98092 16127 15486 9350 9220 76036 14219
5144 2821 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Телеграмма Циммермана, отправленная послом Германии в Вашингтоне своему коллеге в Мексике, Генриху фон Эккардту

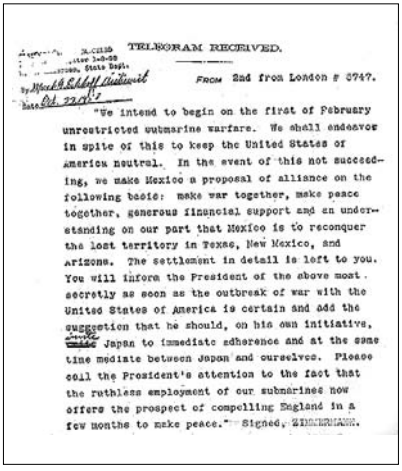
Но Мексике требовалось некоторое время для подготовки своих вооруженных сил. Поэтому было жизненно необходимо, чтобы тайные намерения Германии оставались неизвестными американцам достаточно долго.

Однако у британского правительства были другие планы. Вскоре после начала войны британцы перерезали подводные телеграфные кабели, которые соединяли Германию с западным полушарием напрямую. Таким образом связь должна была осуществляться через другие кабели — те, где британцы могли перехватывать сообщения. США пытались добиться переговоров об окончании войны и поэтому позволяли Германии продолжать передавать дипломатические послания. В результате послание Циммермана было получено немецким посольством в Вашингтоне в целости и сохранности.

Британское правительство отправило перехваченное послание в отдел, занимавшийся дешифровкой и взломом кодов, который назывался «комната № 40».

Немцы использовали свой обычный алгоритм шифрования, которым пользовалось Министерство иностранных дел, а также шифр, известный, как 0075, который эксперты из комнаты № 40 уже частично взломали. Указанный алгоритм включал замену слов (кодирование), а также букв (шифрование). Эта практика была подобна той, которая использовалась

Та же телеграмма, но в расшифрованном виде



TELEGRAM RECEIVED.

From 2nd from London # 8747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of American neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

немцами в еще одном шифровальном инструменте того времени, шифре ADFGVX, который мы более подробно рассмотрим ниже.

Британцам не потребовалось много времени для расшифровки телеграммы. Правда, они не хотели сразу же доводить ее содержание до американцев. Для этого имелись две причины.

Во-первых, секретная телеграмма была отправлена под дипломатическим прикрытием, которое США обеспечивали немецким посланиям, а британцы эту привилегию напрочь проигнорировали. Во-вторых, если бы телеграмму сделали достоянием общественности, то немецкое правительство сразу же узнало бы, что его коды взломаны, и немедленно изменило систему шифровки.

Поэтому британцы решили сообщить американцам, будто бы раздобыли содержание телеграммы, полученной фон Эккардтом, чтобы таким образом убедить немцев, что телеграмма перехвачена уже расшифрованной, в Мексике.

В конце февраля правительство Вильсона передало содержание телеграммы прессе. Некоторые представители прессы, в частности газеты, принадлежащие издательскому дому «Херст» (Hearst), который был настроен против возможной войны и прогермански, вначале отнеслись к ней весьма скептически. Однако к середине марта Циммерман публично признал

авторство противоречивого послания. Чуть более двух недель спустя, 6 апреля 1917 года, Конгресс США объявил войну Германии.

Это решение имело далеко идущие последствия для Европы и мира…

В заключение отметим, что, хотя телеграмма Циммермана и стала чрезвычайным событием своего времени, но это всего лишь одна историческая страничка, в которой важную роль сыграла криптография.

На протяжении этой книги мы увидим немало других примеров, разбросанных по столетиям и культурам.

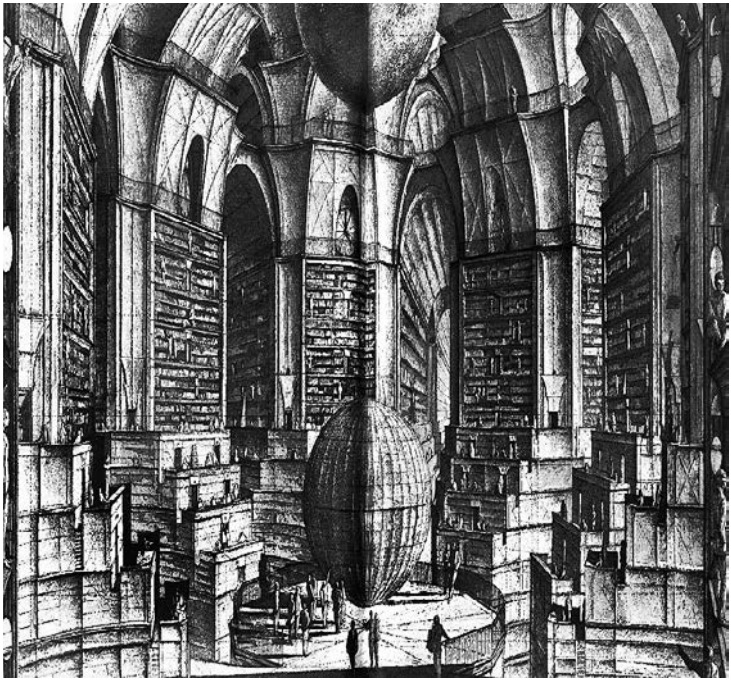
Тем не менее, мы почти наверняка можем утверждать, что далеко не все знаем о самых важных исторических событиях.

Ведь благодаря своей природе история криптографии — это история тайн.

ПОСЛАНИЕ ИЗ ВАВИЛОНА

Аргентинский писатель Хорхе Луис Борхес представил в коротком рассказе «Вавилонская библиотека» такое огромное книгохранилище, что на полках стояли все возможные книги: романы, поэмы и диссертации, а также опровержения этих диссертаций, и опровержения опровержений, и так далее, до бесконечности.

Криптоаналитик, путём проб и ошибок пытающийся расшифровать сообщение, зашифрованное с помощью «одноразового блокнота», столкнётся с подобной же ситуацией. Поскольку шифр полностью произволен, возможная расшифровка будет содержать все возможные тексты той же длины: истинное послание и короткое опровержение послания, и то же самое послание, в котором все правильные существительные заменены другими существительными той же длины, и так далее до бесконечности…



ГЛАВА 2. КРИПТОГРАФИЯ ОТ АНТИЧНЫХ ВРЕМЕН…

«История кодов и шифров — это многовековая история поединка между создателями шифров и теми, кто их взламывает… Трагическая казнь Марии Стюарт, королевы Шотландии, явилась драматической иллюстрацией слабостей одноалфавитной замены; очевидно, что в поединке между криптографами и криптоаналитиками последние одержали верх. Любой, кто отправлял зашифрованное сообщение, должен был отдавать себе отчет, что опытный дешифровальщик противника может перехватить и раскрыть самые ценные секреты».

Сингх Саймон. «Книга шифров»

СКРЫТЫЕ ПОСЛАНИЯ

Древнегреческий учёный Геродот упоминает в своей знаменитой «Истории», посвящённой описанию греко-персидских войн в V веке до н. э., два любопытных случая применения стеганографии, которые свидетельствуют о большой находчивости людей того времени.

В первом примере, который содержится в «Талии», третьей книге «Истории», Гистией, тиран города Милет, приказал одному человеку побрить голову. Затем он написал на бритой голове послание и стал ждать, пока у мужчины снова вырастут волосы. После того как они отросли, посыльного отправили в лагерь Аристагора. Добравшись туда, посыльный объяснил суть дела Аристагору, и волосы снова сбрили, открыв, таким образом, сообщение, которого здесь давно ждали.

Второй пример, если это, конечно, происходило в действительности, имеет гораздо большую историческую важность, поскольку позволил Демарату, царю Спарты, находящемуся в ссылке в Персии, предупредить своих соотечественников о грядущем вторжении персидского царя Ксеркса. Эту историю Геродот рассказывает в «Полигимнии», седьмой книге «Истории»:

> *«Демарат не мог открыто предупредить их, поэтому ему пришла в голову такая мысль: он взял пару табличек [для письма], соскоблил с них воск и написал о планах царя на деревянной поверхности табличек. Затем он снова покрыл их расплавленным воском и таким образом скрыл сообщение. В результате казавшиеся пустыми таблички не вызывали никаких подозрений у стражников в дороге.*
>
> *Когда таблички наконец оказались в Лакедемоне (Спарта), тамошние жители не могли понять,*

в чём тут секрет, пока, насколько я понимаю, Горго […] не предложила соскоблить воск с табличек, потому что под ним — как она подсказала — найдут написанное на дереве послание».

Распространенное стеганографическое средство, которое выдержало испытание временем, — это симпатические (невидимые) чернила. Их применение описано в тысячах рассказов и фильмов. Используемые материалы — лимонный сок, сок растений и даже человеческая моча — обычно органического происхождения и с высоким содержанием углерода. Поэтому высохшие чернила имеют склонность к потемнению, когда оказываются под воздействием умеренно высоких температур, как, например, жар от пламени свечи. Полезность стеганографии нет смысла оспаривать, хотя она делается совершенно непригодной, когда речь идет о больших количествах посланий. Более того, если ее использовать напрямик, без дополнительных ухищрений, у нее обнаруживается существенный недостаток: когда послание однажды все-таки перехватят, содержание его сразу же станет известным. По этой причине стеганография в основном используется как дополнение к криптографии, как средство усиления безопасности сверхсекретных передач.

Во время холодной войны в полных драматизма шпионских триллерах герои часто отправляли послания при помощи средства, на котором буквы оказывались слишком мелкими для чтения невооружённым глазом, — микрофильма. Техника родилась за несколько лет до начала холодной войны, в годы Второй мировой, когда немецкие агенты использовали стеганографическую технику, известную как микрофотоснимок, то есть снимок с очень большим уменьшением. Он состоял из фотографии короткого текста, которая сводилась до размера точки, которую затем включали в виде одного из многочисленных символов в безобидный текст.

Вооруженные конфликты являлись мощным стимулом и побудительным мотивом для развития безопасности информационных сообщений. Поэтому неудивительно, что такие воинственные люди, как спартанцы (если верить Геродоту, они являлись мастерами стеганографии), также стали первопроходцами и в развитии криптографии.