Душкин Роман Викторович
Директор по науке и технологиям Агентства Искусственного Интеллекта

Яхонтов Светозар Игоревич
Директор по развитию компаний StarForce и Safe'n'Sec, эксперт по информационной безопасности.

Стеганография методом Бэкона

Что ж, продолжим... На этот раз мы изучим совершенно новые методы работы с информацией. В предыдущих статьях нашего криптографического цикла мы изучили большое количество методов шифрования информации, но теперь пришло время для методов сокрытия информации. Мы начинаем изучать стеганографию, то есть технологию сокрытия чего бы то ни было среди обыденных вещей. Криптография и стеганография идут рука об руку, как сёстры. И часто зашифрованное каким-либо криптографическим методов послание ещё и сокрыто при помощи стеганографического метода. Так что приступим.

Лучший способ что-то спрятать — это *оставить у всех на виду*. Именно такой способ сокрытия тайных сообщений будет рассмотрен в этой статье.

Фрэнсис Бэкон, автор метода сокрытия тайных сообщений, который мы рассмотрим в этой статье, в первую очередь был политиком. Крупным политиком. В 1618 году Фрэнсис Бэкон, занимая должность лорда-канцлера (аналог современной должности

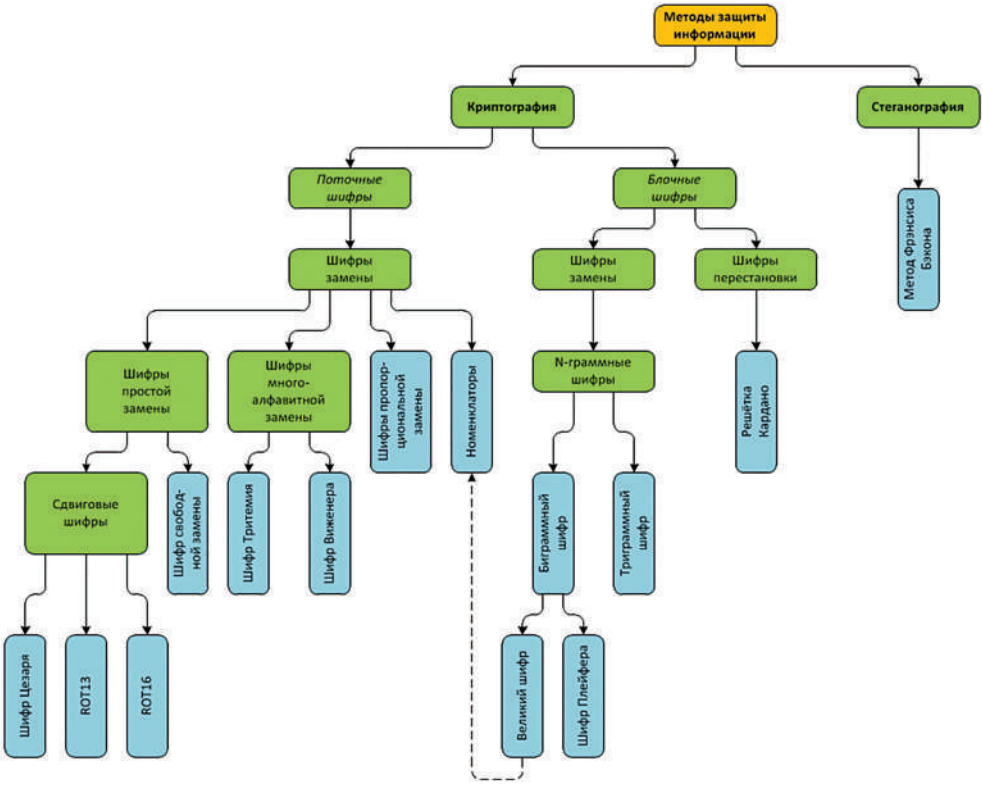
председателя правительства), даже был поставлен в управление Англией на время отбытия короля Якова IV в Шотландию. И добиться такого положения в политике Бэкону позволило, в том числе, его умение хранить тайны.

Важным для построения политической карьеры была возможность первым донести до «ушей короля» (высокопоставленных лордов, приближённых короля) секретов, полученных в результате удачно реализованной интриги. Чаще всего — посредством вхождения в доверие в круг влиятельных политиков с последующим предательством. Передать такой секрет было, зачастую, возможно лишь через посредника, или слугу, который, очевидно, имел все возможности прочитать письмо, и сам был заинтересован в компрометации секрета. Важно было скрыть даже сам факт того, что в передаваемом письме сокрыто тайное послание.

Впервые описание метода сокрытия информации встречается в работе Фрэнсиса Бэкона «О преумножении наук». В своих работах Фрэнсис Бэкон сформулировал три требования, которым должен удовлетворять любой «хороший» шифр. Шифр должен быть:

1. Незамысловатым и несложным в работе.
2. Надёжным и не поддающимся расшифровке.
3. По возможности не вызывать никаких подозрений.

Так что же такое *стеганография*? Это набор методов и практик сокрытия сообщений. Основная



цель стеганографии заключается в том, чтобы скрыть сам факт передачи тайного сообщения. Другими словами, тайное сообщение как бы прячется. Оно даже может быть не шифрованным. Но если спрятанное сообщение ещё и зашифровать каким-нибудь способом, то степень защиты будет повышена, особенно если метод шифрования нарушает частоты распределения символов в шифруемом тексте. Тогда найти стеганограмму намного сложнее, поскольку она начинает выглядеть как «шум». Непосвящённый человек не сможет выявить её, а у криптоаналитика будет очень мало зацепок, чтобы попытаться обнаружить стеганограмму (например, статистическими методами).

Серьёзно дополним нашу схему методов защиты информации.

Метод шифрования

Современный русский алфавит устроен «очень удачно» для этого метода шифрования, так как содержит почти 32 буквы. Конечно, мы используем 33 буквы, но буквы Е и Ё можно рассматривать как одну, равно как и знаки Ъ и Ь тоже можно объединить. И теперь если добавить пробел, у нас получится *ровно* 32 символа. Как мы с вами знаем, в двоичной системе счисления число 32 является «круглым», поскольку в ней оно записывается как 100000. Так что для представления тридцати двух символов нам потребуется 5 бит информации, поскольку $32 = 2^5$. Мы можем воспользоваться этим для нового способа кодирования символов нашего алфавита:

ПРОБЕЛ	00000	**З**	01000	**П**	10000	**Ч**	11000
А	00001	**И**	01001	**Р**	10001	**Ш**	11001
Б	00010	**Й**	01010	**С**	10010	**Щ**	11010
В	00011	**К**	01011	**Т**	10011	**Ъ, Ь**	11011
Г	00100	**Л**	01100	**У**	10100	**Ы**	11100
Д	00101	**М**	01101	**Ф**	10101	**Э**	11101
Е, Ё	00110	**Н**	01110	**Х**	10110	**Ю**	11110
Ж	00111	**О**	01111	**Ц**	10111	**Я**	11111

Каждому символу из алфавита ставится в соответствие пятизначное двоичное число, состоящее ровно из пяти битов 0 или 1. При этом лидирующие нули на первых местах не удаляются, как мы это привыкли делать в десятичной системе. Здесь особенно важно, чтобы длина кода для каждого символа была равна пяти.

Соответственно, чтобы зашифровать текст, необходимо вписать один за другим код каждого символа. Например, пусть есть текст «ИНГРЕДИЕНТЫ ГОТОВЫ». Этот текст шифруется при помощи представленного выше кода так:

01001 01110 00100 10001 00110 00101 01001 00110 01110 10011 11100 00000 00100 01111 10011 01111 00011 11100

А теперь самое главное. Пусть цифра 0 обозначает обычную букву, а цифра 1 — полужирную. Весь этот код можно «нанести» на произвольный текст при помощи такого соответствия. И, самое главное, необязательно использовать свойство жирности символа, для этих целей подойдет любое двоичное свойство: большая или маленькая буква, прямая или курсив, красного цвета или чёрного. Можно даже использовать такие свойства, как «находится в первой половине алфавита или во второй» или «находится на чётном месте в алфавите или на нечётном», но эти два последних свойства сложнее, при помощи их спрятать сообщение можно не в любом тексте.

Как видно, эта же шифрограмма «нанесена» на обычные слова в начале предыдущего абзаца, при этом использовались все символы для нанесения (то есть и цифры, и знаки препинания). Неподготовленный читатель даже не обратит внимание на такое странное начертание текста. И такой способ удобнее применять, если текст будет в последующем распечатан на бумаге на принтере, в этом случае потеря цифрового оригинала текста не будет критичной. Однако, если этот текст будет переписан от руки или на печатной машинке, то тайное сообщение будет утеряно. Для цифровых носителей текста можно использовать более тонкие свойства, которые не так тривиальны, например, использовать два разных похожих шрифта (например, Arial и Calibri).

В одном детективном романе, название которого мы уже не вспомним, важным элементом истории было письмо, написанное героем от руки. В письме было сокрыто сообщение. И двоичным свойством для кодирования сообщения было слитное либо, напротив, раздельное написание букв. Согласитесь, что написанное авторучкой на бумаге таким образом письмо может и вовсе не привлечь внимание читающего. Если только это не учитель русского языка (шутка).

При кодировании текста важно уделить внимание и не пропустить бит (например, 1010 вместо 10101). Иначе это приведёт к сдвигу, в результате которого после расшифровки получится бессмыслица. Конечно, её тоже можно будет расшифровать, так как бессмыслица будет весьма структурированной, однако, это сделает обмен тайными сообщениями не столь удобным для участников тайной переписки.

Методы атаки

Метод атаки на стеганограммы Фрэнсиса Бэкона достаточно прост. Для его применения необходимо:

1. Внимательно смотреть, нет ли в тексте каких-либо странностей в написании символов, которые можно разделить на два класса.
2. Выписать различающиеся написания символов как 0 и 1.
3. Сгруппировать полученные 0 и 1 (например, в группы по 5 битов; но это не обязательно должно быть именно 5 битов).
4. Подобрать возможные алфавиты, закодированные аналогично тому, как представлено в этой статье.

Заключение

Современное применение стеганографии связано не только с сокрытием информации. Стеганография часто применяется для идентификации создателя информации.

Например, когда вы делаете цифровое фото с камеры телефона или фотоаппарата, в файл снимка добавляется информация о модели и серийном номере камеры, дате и времени создании снимка. Это делается для возможности защиты авторского права на снимок. Во всяком случае, так заявляется производителями камер. Но, к примеру, эта информация может использоваться и в целях компрометации. Например, был случай, когда некоего пользователя социальных сетей уличили во лжи из-за того, что умудрённые опытом аналитики изучили геометки в опубликованных им фотографиях, и местоположение съёмки не соответствовало опубликованной ранее информации.

Большинство производителей цветных лазерных принтеров реализовали функциональность печати специальных меток на отпечатанных документах. Эти метки представляют из себя еле заметные жёлтые точки, расположенные на расстоянии 2.5 мм друг от друга. Такими метками закодирована информация о модели и серийном номере принтера, дате и времени печати. Эта функциональность была реализована в сотрудничестве с центральными и национальными банками разных стран с целью противодействия фальшивомонетничеству.

Стеганографию также применяют для контроля доступа к информации. Специальные цифровые метки, «вкрапляемые» в документ, содержат информацию о грифе конфиденциальности (или даже секретности) документа. При попытке открыть такой файл специальные системы сравнивают уровень доступа пользователя и уровень конфиденциальности документа, и, либо позволяют документ открыть, либо блокируют открытие документа с информированием офицера безопасности о попытке несанкционированного доступа к закрытой информации. Также контролируются попытки передать документ за периметр организации (записать на флешку или отправить по электронной почте).

На интернет-форумах и в чатах иногда можно наблюдать обмен картинками невысокого качества. В таких медиафайлах также можно найти скрытые методом стеганографии сообщения. Стеганограмма «прячется» среди «шумов» картинки — малозаметных глазу вкраплений артефактов, которые, при фотосъёмке в условиях недостаточного освещения, проявляются от влияния помех на матрице фотоаппарата, возникающих от локальных токов на подложке матрицы. Достаточно изменить значения последних битов у пикселей на единицу, и на картинке появляется незаметное для человеческого глаза изменение тона пикселей. Отличить такие отклонения от «шумов», просто глядя на картинку, практически невозможно. Однако, эти пиксели уже будут нести в себе то самое двоичное свойство, которое будет частью кода скрытого сообщения. Но об этом мы поговорим в следующий раз.

Мир вокруг нас не так прост, как кажется.

Упражнения

В качестве домашнего задания и самостоятельных упражнений рекомендуем выполнить следующие:

1. Прочитайте следующее произведение:

• Бэкон Ф. *О достоинстве и приумножении наук*

2. Расшифруйте, какое тайное слово сокрыто в первом предложении этой статьи?

3. Самостоятельно зашифруйте какой-либо текст при помощи описанного в статье метода стеганографической защиты, выбрав для этого какое-либо свойство печатных или письменных символов

В журнале «Потенциал» № 7 за 2019 год была опубликована статья этого криптографического цикла «Решётки Кардано». В ней дана формула подсчёта количества возможных вариантов решёток для заданного размера. К сожалению, формула основана на неверной посылке о том, что для подсчёта этого количества необходимо воспользоваться комбинаторным понятием сочетания из N элементов по m. Правильной формулой является следующая:

$$X = 4^{\frac{N^2}{4}}.$$

Эта формула показывает, что количество возможных различных решёток Кардано для заданного размера существенно меньше, чем приведённые в статье, что достаточно снижает криптостойкость приведённого в статье метода шифрования. Авторы благодарят Сергея С. за внимательность.

Новости Новости Новости Новости Новости

Россия подводит итоги своей лунной программы

Россия не была на Луне с 1976 года, но планирует вернуться. В настоящее время агентство Роскосмоса разрабатывает три миссии, которые должны быть развернуты до 2025 года.

Луна очень популярна в наши дни. Упомянем, прежде всего, Соединенные Штаты, которые хотят вернуться на наш спутник в 2024 году в рамках миссий Артемиды, прежде чем поселиться там навсегда в 2028 году. Китай, со своей стороны, также отличился в прошлом году своей миссией "Чанъэ-4", совершив полет на вездеходе по дальнему краю Луны. Не забываем и о миссии "Чанъэ-5", которая должна взлететь в конце года и целью которой будет возвращение образцов луны на Землю. А как же Россия? Российское агентство Роскосмос в настоящее время разрабатывает три лунные миссии под названием « Луна-25», «Луна-26» и «Луна-27», которые начнут с того места, на котором остановилась советская космическая программа в 1970-х годах.

Источник: New-Science.ru https://new-science.ru