Стеганография

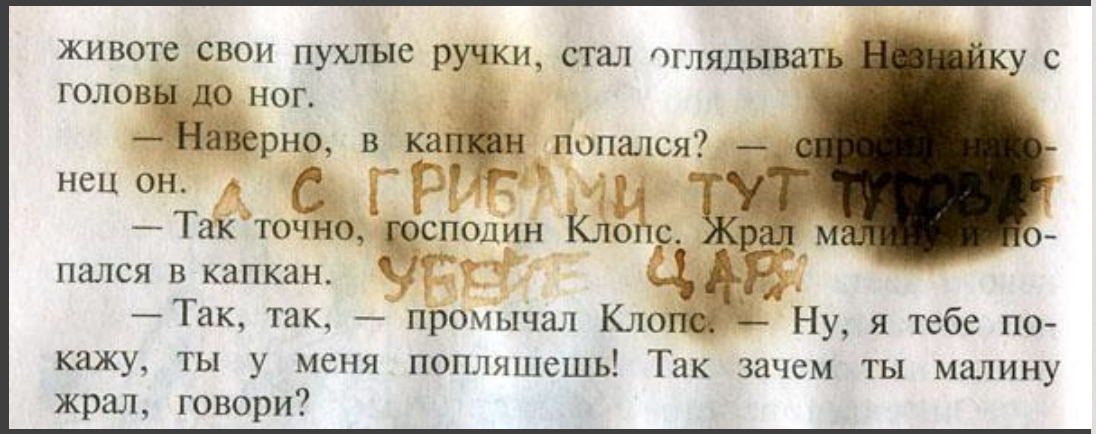
Наука Стеганография

Стеганография – это наука о скрытой передачи информации путем сохранения в тайне самого факта передачи.

Исторические факты применения Стеганографии

С восковой дощечки соскабливали воск,
затем ,царапали прямо на дереве секретное послание,
после покрывали воском и писали уже на воске открытое письмо
Использовали в Древнем Риме.

Ленин , находясь в заключении ,писал свои труды молоком наливая его в «чернильницу» из хлебного мякиша которую при опасности съедал. Листы , исписанные таким образом ,передавались на волю ,там листы нагревали над лампой или свечой и переписывались сопартийцами.


животе свои пухлые ручки, стал оглядывать Незнайку с головы до ног.

— Наверно, в капкан попался? — спросил наконец он.

— Так точно, господин Клопс. Жрал малину и попался в капкан.

— Так, так, — промычал Клопс. — Ну, я тебе покажу, ты у меня попляшешь! Так зачем ты малину жрал, говори?

«Микроточка»

При увеличении «микроточка» дает изображение печатной страницы , чертежей, рисунков.

Конверт с микроточкой, отправленный в 1941 г. немецкому агенту в США

Классификация Стеганографии

В конце 90х годов выделились несколько направлений стеганографии:

Классическая стеганография-включает в себя **«некомпьютерные методы»**

Компьютерная стеганография – направление классической стеганографии , основанное на особенностях компьютерной платформы и использования специальных свойств компьютерных форматов данных.

Цифровая стеганография - направление классической стеганографии , основанное на сокрытии или внедрении дополнительной информации в цифровые объекты , вызывая при этом некоторые искажения этих объектов .

Основные задачи стеганографии

Защита конфиденциальной информации от несанкционированного доступа;

Преодоление систем мониторинга и управления сетевыми ресурсами;

Камуфлирование программного обеспечения;

Защита авторского права на некоторые виды интеллектуальной собственности.

Основные понятия

Стеганографическая система или стегосистема - совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

Контейнер - любая информация, предназначенная для сокрытия тайных сообщений.

Пустой контейнер - контейнер без встроенного сообщения; заполненный контейнер или стего - контейнер, содержащий встроенную информацию.

Встроенное (скрытое) сообщение - сообщение, встраиваемое в контейнер.

Стеганографический канал или просто стегоканал - канал передачи стего.

Стегоключ или просто ключ - секретный ключ, необходимый для сокрытия информации. В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей.

Стеганографическая система или стегосистема

Атаки на стегосистемы

Атака на основе известного заполненного контейнера.

Атака на основе известного встроенного сообщения.

Атака на основе выбранного скрытого сообщения.

Адаптивная атака на основе выбранного скрытого сообщения.

Атака на основе выбранного заполненного контейнера.

Атака на основе известного пустого контейнера.

Атака на основе выбранного пустого контейнера.

Атака на основе известной математической модели контейнера или его части.

Методы компьютерной стеганографии

Использование зарезервированных для расширения полей компьютерных форматов данных.

Один из методов специального форматирования текстовых файлов

Из специального форматирования

Из группы специального форматирования текста

Скрытие в неиспользуемых местах гибких дисков

Использование имитирующих функций

Удаление заголовка идентифицирующего файл

Группа методов использования избыточности аудио- и визуальной информации.

Использование избыточной цифровой фотографии

Использование избыточности цифрового звука.

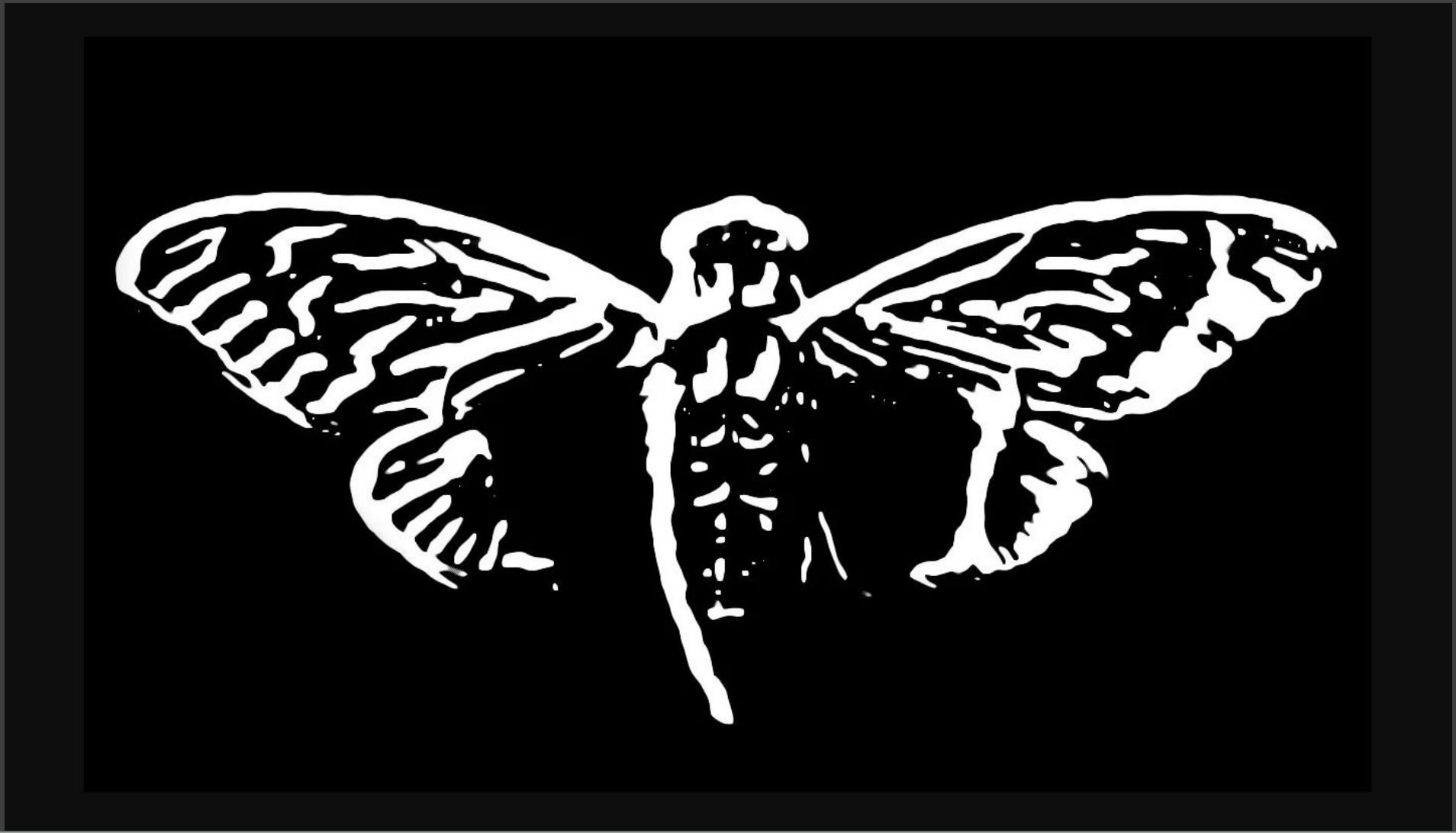
Метод наименее значащих битов (Least Significant Bit, LSB)

Стеганографическая система или стегосистема

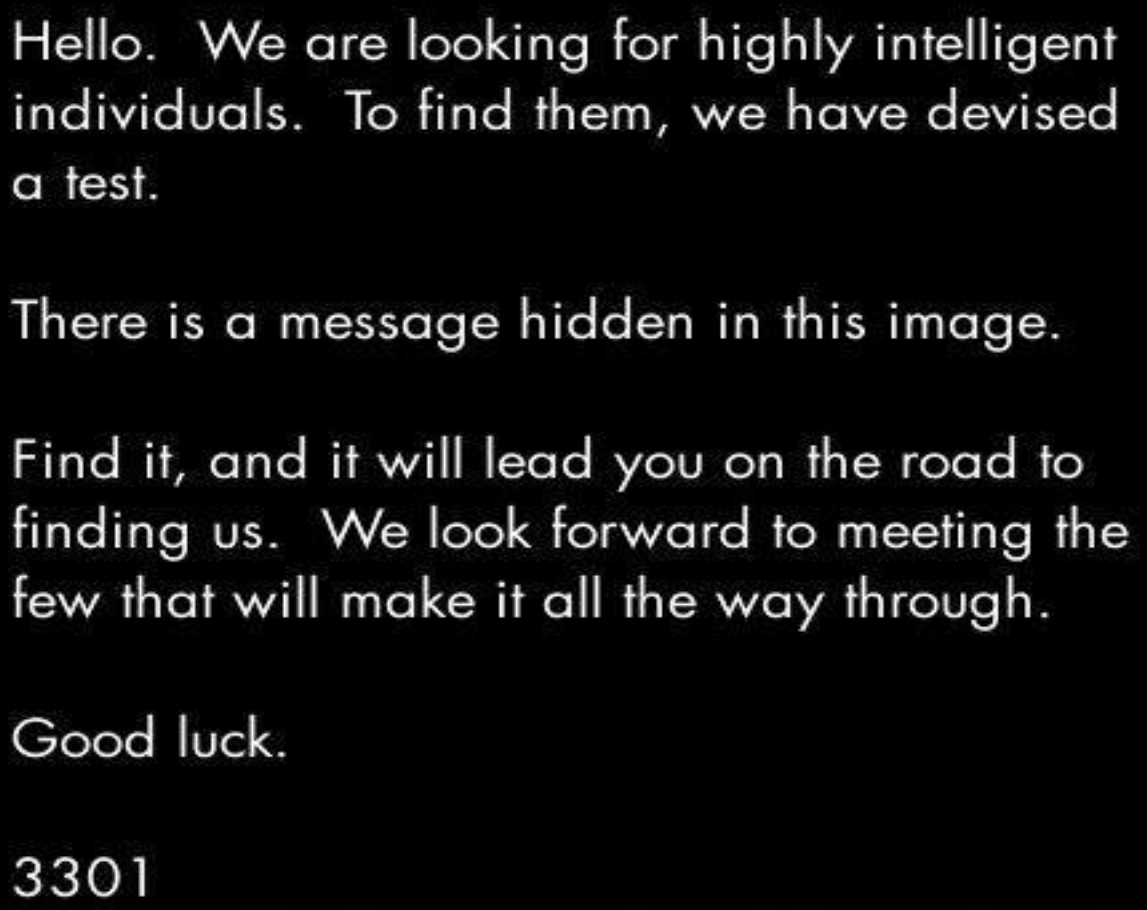
Заданий у меня для вас нет ,поэтому хочу предложить кое-что тоже

довольно интересное ⏺

Интригует ?



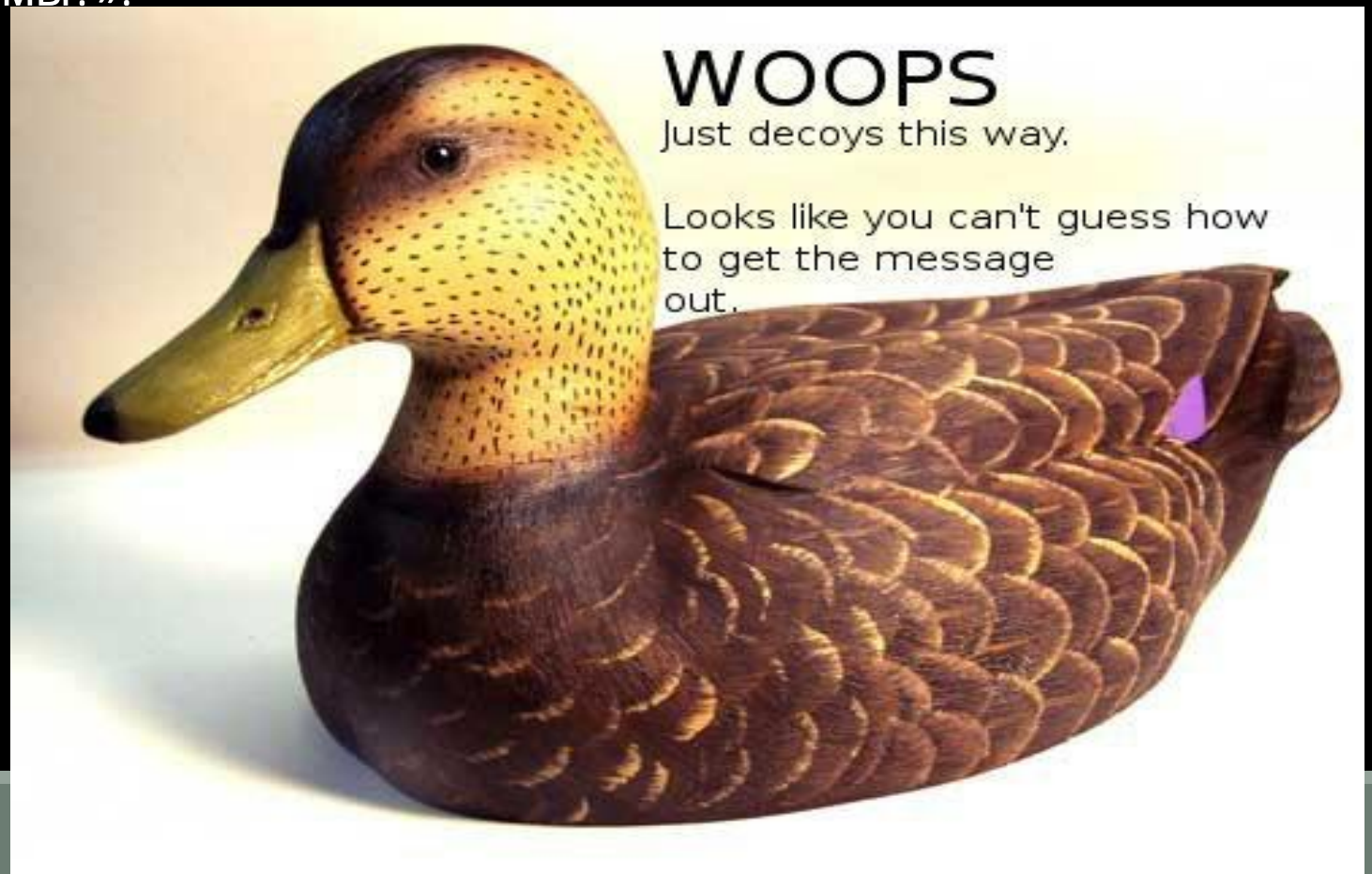
Всё началось 4 января 2012 года, когда посетители всем известного 4chan обнаружили пост с картинкой, представлявшей собой белый печатный текст на чёрном фоне.



Текст гласил: «Привет. Мы ищем лиц с высоким интеллектом. Для этого мы разработали тест. В этом изображении есть скрытое сообщение. Найдите его, и оно покажет вам, как найти нас. С нетерпением ожидаем тех немногих, которым удастся пройти весь путь. Удачи. 3301».

Кто-то из комментаторов предложил открыть изображение в простом текстовом редакторе WordPad, и в полученном тексте обнаружилось единственное осмысленное сообщение: «TIBERIVS CLAVDIVS CAESAR says «lxxt>33m2mqkyv2gsq3q=w]O2ntk»», то есть «Тиберий Клавдий Цезарь говорит “lxxt>33m2mqkyv2gsq3q=w]O2ntk”». Благодаря очевидной подсказке расшифровать код оказалось несложно: это был так называемый код Цезаря, или шифр сдвига, в котором каждый отдельный символ в тексте заменяется символом, находящемся в алфавите на некоторое постоянное число позиций левее или правее. Для знающих, что Тиберий Клавдий был четвёртым римским императором, было логичным предположить, что сработает смещение текста на четыре буквы назад, — результатом которого и стал адрес сайта в интернете.

Зашедшего по этому адресу встречало изображение утки с издевательской надписью: «УПС просто заманивает сюда. Похоже, вы не смогли догадаться, как извлечь сообщение». Ключ к загадке скрывался в английском тексте: слова «guess» и «out» приводили к названию стеганографической программы OutGuess, позволяющей выявлять данные, которые скрыты в обычных цифровых изображениях. Прогнав картинку через OutGuess, можно было получить последовательность цифр с пометкой «Это книжный код» и ссылку на одну из «досок» популярного сайта Reddit, где посетителя встречали код, который состоял из цифр, использовавшихся в древности индейцами майя, множество периодически добавляющихся зашифрованных строчек и две картинки с надписями «Добро пожаловать» и «Проблемы?».



В каждой картинке было скрыто по сообщению, которые также можно было прочитать с помощью OutGuess. В первом говорилось, что с этого момента каждое послание будет иметь PGP-подпись, и приводилась эта подпись, а второе гласило: «Ключ был всегда перед вашими глазами. Это не поиски Священного Грааля. Перестаньте всё усложнять. Удачи. 3301».

Цифры майя были ключом к расшифровке строчек: здесь снова использовался код Цезаря, и в результате перед глазами представал отрывок из поэмы о короле Артуре, входящей в состав средневекового валлийского сборника повестей «Мабиногион». Применив к расшифрованным строчкам «книжный код», дававшийся ранее (первое число — номер строки, второе — порядковый номер буквы), можно было получить такой текст: «Call us at us tele phone numBer two one four three nine oh nine six oh eight», то есть «Позвоните нам по телефонному номеру 2143909608».

Трубку снимал автоответчик с таким сообщением: «Очень хорошо. Вы справились. Три простых числа связаны с оригинальным изображением final.jpg. 3301 одно из них. Вы должны найти другие два. Чтобы перейти на следующий уровень, перемножьте эти числа между собой и добавьте .com. Удачи. До свидания».

Размеры первоначального изображения составляли 509×503 пикселя, и оба этих числа простые. Перемножив их с 3301, можно было получить адрес 845145127.com, где посетителя встречало изображение цикады и счётчик с обратным отсчётом.

Очередное сообщение, скрытое в картинке, гласило: «Вы хорошо постарались, чтобы зайти так далеко. Терпение — это добродетель. Вернитесь сюда в 17:00 в понедельник 9 января 2012 года по всемирному времени».

После того как отсчёт прекратился, сайт обновился, и в изображении цикады было скрыто уже другое сообщение, содержащее 14 GPS-координат разных точек на земном шаре, включая Варшаву, Париж, Сиэтл, Сеул, Аризону, Калифорнию, Новый Орлеан, Майами, Гавайи и Сидней. Масштабы мероприятия поразили даже самых недоверчивых участников!

По всем указанным адресам находились уличные фонарные столбы, к которым был прикреплён плакат с изображением цикады и QR-кодом. Различные варианты сообщений предлагали расшифровать очередной «книжный код», на сей раз в книге «Агриппа» Уильяма Гибсона, который в итоге приводил к адресу sq6wmgv2zcsrix6t.onion в сети TOR. Подавляющее большинство зашедших по этому адресу получали сообщение «Нам нужны лучшие, а не последователи», а несколько недель спустя на 4chan и Reddit появилось следующее: «Привет. Мы нашли тех, кого искали. Так наше путешествие длиной в месяц заканчивается. Пока».

Спасибо за внимание !