электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.056.55

Шифрование информации на основе эффекта Талбота

***Щетинин Г.А.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Программное обеспечение ЭВМ и информационные технологии»

Научные руководители: Романова Т.Н., к.ф.-м.н., доцент
кафедра «Программное обеспечение ЭВМ и информационные технологии»
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана

Скуйбин Б.Г., к.ф.-м.н., доцент
кафедра «Физика»,
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
rtn@bmstu.ru

В современном мире всё большую роль играет необходимость защиты определенной информации от несанкционированного доступа. Это может быть самая разная информация: логины и пароли на школьных сайтах подготовки к экзаменам, пароли от банковских карт, личная переписка и многое другое. В современном мире также существует множество алгоритмов шифрования с различной степенью сложности. В алгоритме[1], [2], [3] ключ состоит из 256 битов, а пространство ключей из 2^{256} бит. Если используются слабые ключи, то их можно вскрыть, имея, например, 4 пары «открытый» - «закрытый» текст, а если в алгоритме используются сильные ключи – то 2^{64} пар. В то же время растут возможности вычислительной техники – отсюда возникает необходимость создания более сложных уникальных алгоритмов шифрования.

Разработанный алгоритм на основе эффекта Талбота (и созданная на его основании компьютерная программа) позволяют шифровать текст или бинарный код довольно большого объема, а также расшифровать полученную информацию в виде текста или бинарного кода.

Явление саморепродукции – явление периодического самовоспроизведения изображения предмета, освещенного плоской монохроматической волной без использования фокусирующих/преломляющих оптических приборов, на некотором расстоянии от предмета. Это эффект (позже названный эффектом Талбота) изучал Рэлей: он получил формулу для расчета длины Z_T, которую назвали длиной Талбота. Подробно

изучение дробного эффекта Талбота и создание компьютерной модели изложено в статьях[4], [5], [6], [7], [8] и [9].

На дробных расстояниях Талбота Z:

$$Z = \frac{n}{2 * m} Z_T \qquad (1),$$

где n и m – целые числа, период и фаза изображения изменяются по следующим формулам:

$$d_Z = \frac{d}{m} \qquad (2)$$

$$\varphi_Z = 2 * \pi * n \qquad (3),$$

где d_Z, φ_Z – период и фаза соответственно изображения на дробном расстоянии Талбота,

d - период исходной дифракционной решетки.

Основные шаги алгоритма шифрования текста:

1) Текст разбивается на произвольное число блоков: максимальное число блоков задается шифровальщиком.

2) Каждый блок, состоящий из символов, записывается в виде бинарного кода.

3) Из бинарного кода создается дифракционная решетка со светлыми и темными отверстиями.

4) На полученную дифракционную решетку падает свет. На произвольном дробном расстоянии Талбота берется сечение ковра Талбота.

5) Шаги 2-4 повторяются для каждого блока.

6) Блоки передаются в произвольном порядке.

Стоит отметить, что шифрование дважды одной и той же информации даст разный результат (может варьироваться как число «блоков», так и свет, падающий на дифракционную решетку, дробное расстояние Талбота и некоторые другие параметры).

Таким образом, для того чтобы расшифровать полученную в виде изображений сечения ковра Талбота информацию необходимо знать:

- порядок передачи блоков;
- дробное расстояние, на котором построено сечение ковра Талбота
- ключи к алгоритму создания дифракционной решетки из бинарного кода

Дешифровщик может получить эти ключи двумя способами: либо ключи ему известны заранее (или их ему сообщили по другому каналу связи) или ключи также зашифрованы и переданы с остальным текстом. В разработанном алгоритме используются оба способа. Первые два пункта шифруются с помощью предлагаемого алгоритма и полученные изображения «смешиваются» с исходной информацией, а третий пункт передается через длину волны, падающей на дифракционную решетку. Дешифровщик в зависимости от длины волны может применить соответствующие ключи воссоздания бинарного кода из рисунка дифракционной решетки.

Остается определить только способ, как дешифровщик узнает, какие блоки содержат «исходную информацию», а какие – ключи. Эту информацию (а именно номера блоков) необходимо передавать по другому каналу связи.

Приведем пример работы алгоритма: возьмём всем известный текст из фильма «Семнадцать мгновений весны»:

«Центр - Юстасу

По нашим сведениям, в Швеции и Швейцарии появлялись высшие офицеры службы безопасности СД и СС, которые пытались установить контакт с работниками Алена Даллеса. Вам необходимо выяснить, являются ли эти попытки контактов:

1. дезинформацией,

2. личной инициативой высших офицеров СС и СД,

3. выполнением задания Центра.

В случае если эти сотрудники СД и СС выполняют задание Берлина, необходимо выяснить, кто послал их с этим заданием конкретно: кто из высших руководителей Рейха ищет контакт с Западом.

Алекс»

Если задать в качестве исходных данных для максимального количества элементов в «блоках» равное 50, то получаем набор изображений (приведенный на рисунке 1), полученный в результате шифрования приведенного выше текста с использованием одного набора чисел полученного с помощью генератора случайных чисел:

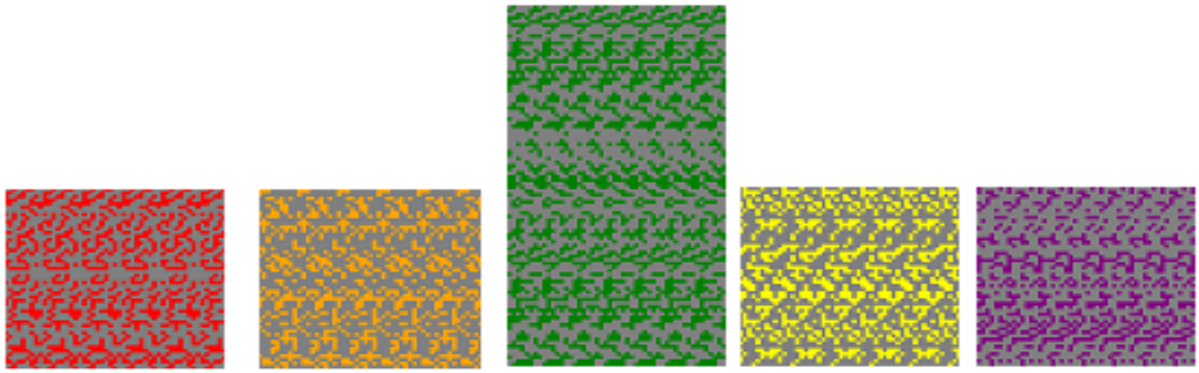

Рис. 1. Первый результат шифрования

На рисунке 2 представлен второй вариант шифрования того же текста, полученный в результате шифрования приведенного выше текста с использованием другого набора чисел полученного с помощью генератора случайных чисел:

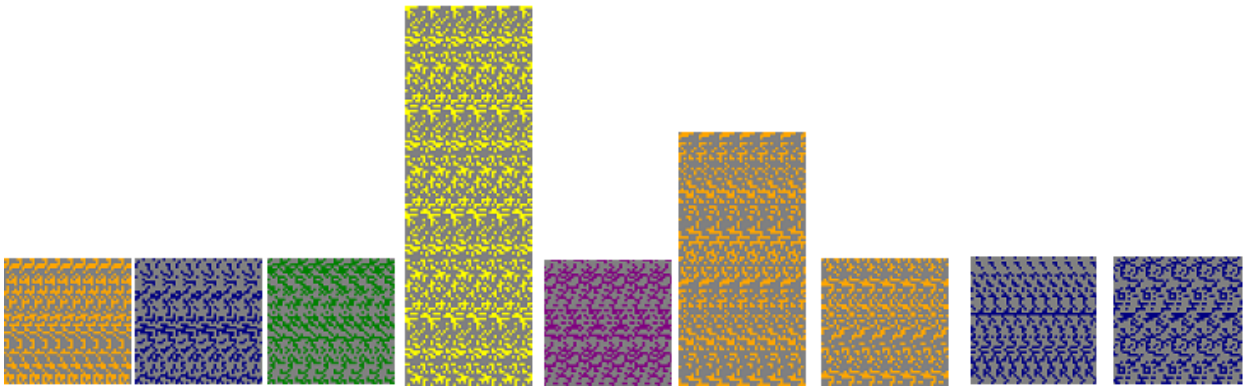

Рис. 2. Второй результат шифрования

Оценим сложность предлагаемого алгоритма:

1. Предположим, что информация зашифрована в N изображениях.
2. Не зная, какой из блоков описывает порядок следования блоков, придется перебрать N! вариантов порядка следования блоков.
3. Не зная дробные расстояния Талбота, на которых взяты данные сечения, придется перебрать (как минимум) 128 вариантов для каждого блока (кроме 2-х первых, которые считаются блоками «порядка» и «дробных расстояний»).

Таким образом, не зная ключи для расшифровки информации, передаваемой предлагаемым алгоритмом необходимо перебрать вплоть до 2^7 N! вариантов. Кроме того, для каждого из этих вариантов надо воссоздать текст из дифракционных решеток. Таким образом, сложность ещё больше возрастает.

Перспективы развития алгоритма и программы: протестировать алгоритм в различных вариантах использования и проверить степень криптоустойчивости. Исследовать алгоритм и программу на возможные взаимодействия с различными видами хакерских атак (вирусы: троянские кони, черви, снифферы; защита от навязывания ложных данных, атак скольжения и атак отражения).

Список литературы

1. ГОСТ 28147-89: Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Режим доступа: http://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=131282 (дата обращения 24.03.15).
2. ГОСТ 28147-89: Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Режим доступа: http://rsdn.ru/article/crypto/gost28147_1.xml (дата обращения 24.03.15).
3. ГОСТ 28147-89: Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Режим доступа: https://ru.wikipedia.org/wiki/%C3%CE%D1%D2_28147-89 (дата обращения 24.03.15)
4. Скуйбин Б.Г., Смирнов Е.В. Эффект Талбота I. Дифракция на одномерных решетках // Физическое образование в ВУЗах. 2014. Т.20. № 2. С. 109.
5. Смирнов Е.В., Скуйбин Б.Г. Дифракция Френеля на пропускающих решетках. Эффект Тальбота // Восьмая Всероссийская конференция: «Необратимые процессы в природе и технике»: труды в 3 частях. Часть III. М.: МГТУ им. Н.Э. Баумана, 2015. С. 202-205.
6. Романова Т.Н., Скуйбин Б.Г., Щетинин Г.А. Трехмерный программный симулятор физического эффекта эксперимента «эффект Талбота» // Восьмая Всероссийская конференция: «Необратимые процессы в природе и технике»: труды. В 3 ч. Ч. III. М.: МГТУ им. Н.Э. Баумана, 2015. С. 226-229
7. Щетинин Г.А., Романова Т.Н., Скуйбин Б.Г. Исследование физического эксперимента «эффект Талбота» с использованием компьютерной модели // Молодежный научно-технический вестник. Электрон. журн. МГТУ им. Н.Э. Баумана № 12. 2014. Режим доступа: http://sntbul.bmstu.ru/doc/746277.html (дата обращения 17.02.15).
8. Щетинин Г.А., Романова Т.Н., Скуйбин Б.Г. Компьютерная модель эффекта Талбота // Молодежный научно-технический вестник. Электрон. журн. МГТУ им. Н.Э. Баумана № 1. 2015. Режим доступа: http://sntbul.bmstu.ru/doc/753130.html (дата обращения 17.02.15).

9. Романова Т.Н., Скуйбин Б.Г., Щетинин Г.А. Программный симулятор физических экспериментов на основе эффекта Талбота // XIII международная научно-практическая конференция NIDays - 2014: «Инженерные и научные приложения на базе технологий NI»: сборник трудов. М.: ДМК Пресс, 2014. С. 410 – 412.