Создание онлайн-среды по криптографии и оценке криптостойкости

Марков Я.А.

Информатика

9 класс, Предуниверситарий НИУЯ МИФИ, университетский лицей №1523, г.Москва, cyberbugz@yandex.ru

Научный руководитель: Троицкий И.И. МГТУ им. Н.Э. Баумана

Введение

Тема использования прикладных криптографических решений в реальной жизни очень востребована. В некоторых важных областях криптография является обязательной. В бытовом плане криптографию используют для хранения секретов (паролей, пин-кодов), защиты персональных данных (фотографий, справок, личных дневников), передачи данных в закрытом виде (например, передать пароль или ответ на квест в школьном чате). В обычной жизни компьютер можно потерять или его могут украсть, но важные данные злоумышленник не сможет прочитать, если они зашифрованы. В настоящее время современную криптографию разделяют на симметричную и асимметричную. При этом зачастую забывают про классические шифры. Однако классические шифры продолжают играть важную роль в нашей жизни.

Во-первых, симметричные шифры и дисковые шифровальные машины созданы на основе классической криптографии с одним ключом.

Во-вторых, многие классические шифры активно используются в сфере ИТ. Так, многие устройства (например, CISCO) используют для скрытия программного кода именно шифр Цезаря.

В-третьих, только для варианта классического шифра Вернама (одноразовый блокнот) доказана абсолютная стойкость шифра и его используют для защиты важных документов. Многие удаленные объекты (космические аппараты, дрейфующие станции), где затруднено обновление ключей, используют именно классические шифры высокой стойкости.

И наконец, классические шифры доступны, их использование не требует особых разрешений, лицензий и сертификаций! Можно добавить, что указанные шифры широко используются при обучении во многих предметах, например, в логике, кибернетике, информационной безопасности, информатике.

Это обусловило идею по созданию веб-сайта по изучению классических шифров. Анализ подобных исследований показал ряд недостатков, например:

- основное внимание уделяется шифрованию и расшифрованию, то есть опускается вопрос проверки стойкости шифров (дешифрованию);

- как оказалось, популярный частотный анализ не позволяет расшифровать короткие фразы, а, как известно, прямой перебор может быть очень длительным.

ОСНОВНАЯ ЧАСТЬ

Цели и задачи научно-исследовательской работы

В работе под криптографией понимаются методы по шифрованию, расшифрованию, а также по дешифрованию. Под шифрованием понимается способ перевода читаемых данных в нечитаемый вид, а под расшифрованием, соответственно, перевод обратно. В классическом шифровании используются два понятия: алгоритм шифрования и ключ шифрования. В таком случае ключ используется и для шифрования, и для расшифрования. Дешифрование – это проверка, как легко взломать шифр. В результате дешифрования делается попытка подобрать ключ [1].

Целью работы является создание сайта с работающими в онлайн-режиме программами по криптографии. В работе решаются следующие три задачи:

1. Написать и проверить программы на JavaScript по шифрованию, по расшифрованию и по дешифрованию;

2. Провести исследование методов дешифрования и разработать эффективный подход к дешифрованию;

3. Сделать веб-сайт и разместить там программы по криптографии.

Разработка программ по шифрованию и расшифрованию

Конструкторская часть работы включает решение задач по программированию. Для начального исследования были выбраны популярные

классические шифры, как перестановочные (обобщенный шифр Цезаря и диск Альберти), так и перестановочные (шифр Атбаш и шифр Вернама). Выбор шифров в каждом классе был определен требованием от «простого к сложному»!

Наиболее известным является шифр Цезаря. Как известно, Цезарь использовал сдвиг на три символа на латинице, а обобщенный алгоритм допускает различные алфавиты и сдвиги. Здесь ключом является сдвиг.

Диск Альберти - это развитие шифра Цезаря, когда сдвиг очередного символа меняется в соответствии с ключом (ключ задает несколько сдвигов). Диск Альберти является аналогом современных дисковых устройств по шифрованию!

Шифр Атбаш – это популярный подстановочный шифр, в котором правило подстановки определяется заменой по правилу обратной индексации символов в алфавите.

Шифр Вернама - это шифр, в котором символы исходного текста складываются по правилу XOR с символами ключа. Если ключ больше или равен длине открытого текста, то считается (согласно теореме Клода Шеннона), что шифр взломать нельзя.

В рамках исследования разработаны соответствующие программы на языке JavaScript (рис. 1).

Рис. 1. QR-коды для шифрования и расшифрования

Исследование программ дешифрования

Исследовательская часть состоит в анализе методов шифрования и разработке подхода, исключающего их недостатки. В литературе описаны несколько методов дешифрования. В работе исследовано три:

- прямой перебор;

- дешифрованием по известной фразе;

- частотный анализ.

Выбор обоснован следующим:

1. Прямой перебор подразумевает подбор всевозможных ключей. Определено, что эффективность любых других способов дешифрования интерпретируется относительно прямого перебора. Можно продемонстрировать трудоемкость перебора, например, ключ из 8 символов имеет почти квинтиллион комбинаций[1]. Для реализации прямого перебора такого ключа потребуется супервычислитель.

2. Дешифрование по известной фразе упрощает криптоанализ. Примером может служить методика взлома немецких шифров времен II мировой войны - «Eins-алгоритм», предложенный математиком Аланом Тьюрингом, который заметил, что в немецких шифртелеграммах наиболее часто употребляется немецкое слово «один» (eins)[1].

3. Что касается частотного анализа, то считается, что такой анализ, как считается, позволяет дешифровать любой классически шифр[2]. Суть частотного анализа состоит в том, что рассчитывается частота употребления букв алфавита, а при дешифровании символы зашифрованного текста заменяются в соответствии с частотой их использования. К примеру, в интернет доступны словари частотности русских букв[3] и других символов[4].

Разработка программ по дешифрованию

Исследуемый частотный анализ показал неэффективность при небольших сообщениях (табл. 1). По сути, частотный анализ начинает выдавать воспринимаемый результат с 4-6 тыс. символов. Кстати, автор доказал, что художественный пример в книге Конан Дойла «Пляшущие человечки» не мог быть решен методом частотного анализа (Шерлок Холмс отгадал всего одну букву Е, при этом 2-ая предполагаемая им буква Т ввела бы его в заблуждение).

---

[1] При алфавите, который включает латиницу (52), кириллицу (66), цифры (10), знаки и спецсимволы (40) число комбинаций равно 168^8 ($6.4*10^{17}$).

[2] Метод упоминается в книгах Конан Дойля и Жюль Верна для расшифровки различной тайнописи.

[3] https://ru.wikipedia.org/wiki/Частотность

[4] https://www.bckelk.org.uk/words/etaoin.html

Таблица 1.

Пример применения частотного анализа

Набор часто используемых слов	Результат частотного анализа 200 символов	Результат частотного анализа 5 тыс символов
не на что как он по	не на фло йай он то	не на что как он до
из это от за же но	ид зло ол да уе но	вз это от за же но
для так бы только она	пр, лай мя лорьйо она	шля так бы только она
или еще мы до уже они	ири есе ыя по буе они	влв еще мы шо уже онв
когда ни чтобы быть	йогпа ни фломя мяль	когша нв чтобы быть
ты время есть даже вы	ля цвеы, е.ль пауе ця	ты премя есть шаже пы
если очень себя под	е.ри офень .ем, топ	еслв очень себя дош
чем где без нет раз	феы гпе мед нел вад	чем гше без нет раз
вот том можно да	цол лоы ыоуно па	пот том можно ша
более там **человек**	морее лаы **фероцей**	более там **челопек**

Разработка экспертного алгоритма и оценка его эффективности

Как указывалось, исследование развеяло миф, что частотный анализ позволяет взломать любой классический шифр. На деле его результативность резко падает при уменьшении исходного текста.

В исследовании была сформулирована гипотеза, что при подборе статистик можно угадать символы в зашифрованной фразе. Поэтому в рамках исследования был придуман эвристический частотный анализ. Суть его состоит в генерации множества статистик. При этом расшифровки с помощью данных статистик сравниваются с набором наиболее часто используемых 10 000 слов (рис. 2). Эксперимент показал, что фрагмент текста в 200 символов начинает восприниматься аналитиком от 500 генераций и более (табл.2). В настоящее время в интернет не найдено аналога подобного алгоритма.

Рис. 2. QR-код для дешифрования методом эвристического частотного анализа

Таблица 2.

Пример применения эвристического частотного анализа

Пример (200 символов)	Число статистик	Расшифровка
не на что как он по из это от за же но для так бы только она или еще мы до уже они когда ни чтобы	1	не на фло йай он то ид зло ол да уе но пр, лай мя лорьйо она ири есе ыя по буе они йогпа ни фломя мяль ля цвеы, е.ль пауе ця е.ри офень .ем, топ феы гпе мед нел вад цол лоы ыоуно па морее лаы **фероцей**
быть ты время есть даже вы если очень себя под чем где без нет раз вот том можно да более там **человек**	500	не на что как он по из это от за же но дхя так бы тохько она ихи еще мы до уже они когда ни чтобы быть ты время есть даже вы есхи очень себя под чем где без нет раз вот том можно да бохее там **чеховек**

Разработка веб-сайта

В рамках исследования автором был зарегистрирован домен cyberbugz.ru. А сам сайт был запрограммирован в среде WordPress. Выбор WordPress был определен не только популярностью, но и удобными функциями по управлению сайтом, разнообразием плагинов, возможностью разграничения функций администраторов, системными возможностями и пр.

Обзор литературы, новизна, достоверность

В электронной библиотеке elibrary.ru было найдено 25 научные статьи по анализу классических шифров[5], однако доступный текст статей представлен лишь в [2-12]. Во всех статьях рассмотрены лишь вопросы шифрования и расшифрования, причем большинство затрагивают только шифр Цезаря. По сути, в интернет отсутствует предлагаемый автором вариант обеспечения шифра тремя составляющими: шифрование, расшифрование и дешифрование [13]. В [4 и 13] было проведено исследование взлома шифра Цезаря методом перебора на

[5] https://www.elibrary.ru/keyword_items.asp?id=9844820

языке Python. Следует отметить, что в интернет дано описание метода (на языке Python) частотного анализа на сайте www.habr.com [14], выполненное в сравнении с информацией, данной в Википедии[6], однако и в нем есть недостатки (учтены лишь буквы русского языка, не рассмотрен способ использования частотного анализа при переборе - не был просчитан пробел). Доказано, что данный метод не работает для небольших сообщений [13].

Исходя из этого, разработан оригинальный метод дешифрования, сочетающий частотный анализ (с генерацией статистик [15]) и проверку по наиболее используемым фразам. Достоверность и практическая значимость исследования подтверждена доступностью веб-сайта, на котором представлены разработанные программы.

ЗАКЛЮЧЕНИЕ

Таким образом, в работе создан оригинальный веб-сайт с криптографическими программами, в том числе:

1. Разработаны программы для шифрования, расшифрования, дешифрования (программы прямого перебора и интеллектуального поиска).

2. В работе разработан оригинальный метод дешифрования, сочетающий частотный анализ и проверку по наиболее используемым фразам.

3. Создан сайт, посвященный тематике безопасности информации.

В рамках исследования были сделаны следующие выводы:

Оказалось, что частотный анализ малорезультативен при дешифровании шифртекста до 5 тыс. символов. Для исключения данного недостатка впервые предложен способ повышения эффективности частотного анализа шифров, основанный на генерации статистик и сравнения с 10 000 наиболее часто встречающимися словами. Эффективность предложенного метода определяется количеством сгенерированных статистик и доступными вычислительными ресурсами

[6] https://ru.wikipedia.org/wiki/Частотный_анализ

Проведенное исследование и разработанный веб-портал, думается, будут полезны старшим школьникам и студентам, увлеченным анализом проблем кибербезопасности и криптографии.

Список литературы

1. Семь безопасных информационных технологий / А.В.Барабанов и др. – М.: ДМК пресс, 2017. – 224 с.

2. Адаев Р. Б. Программная реализация шифрования текстовых фраз // Инженерный вестник Дона. 2021. № 11 (83). С. 172-180.

3. Ачекеев К.С. и др. Создание компьютерной программы для шифрования текстовой информации // Известия ВУЗов Кыргызстана. - 2022. - № 2. - С. 45-47.

4. Гумерова Л.З. и др. Взлом шифра Цезаря методом «грубой силы» // В сб. II Всероссийской научно-практической конференции «Лучшие практики общего и дополнительного образования по естественно-научным и техническим дисциплинам». - Казань: Казанский (Приволжский) Федеральный университет, 2022. С. 157-163.

5. Змейкина А.А., Сунгатов И.З. Экспертная система "Шифр Цезаря" // Сб. научных статей Международной научно-технической конференции «Современные инновации в технике и технологиях» - Курск: "Университетская книга", 2025. – С. 129-132.

6. Карпенкова Н.В. Использование модулярной математики в криптографии // Электронный научно-практический журнал Культура и образование. - 2015. - № 1 (17). - С. 26.

7. Кузьминых Е.С., Маслова М.А. Анализ симметричных методов шифрования, проблемы и пути возможного их решения // Научный результат. Информационные технологии. 2023. Т. 8. -№ 1. - С. 38-45.

8. Лепшокова А.Р. Разработка интерактивного приложения для наглядного представления шифра Цезаря // В сб. Международной научно-практической конференции «Актуальные проблемы методики обучения информатике и математике в современной школе». М.:МПГУ, 2020. С. 493-498.

9. Матвеева А. С. Реализация системы удаленного выполнения команд с использованием шифрования // Постулат. – 2025. – № 1(111). С. 1-8.

10. Михаэлис В.В., Михаэлис С.И. Шифрование в среде MS Excel для безопасной передачи и хранения данных // Современная наука: актуальные проблемы теории и практики. - 2023. - №04/2. - С. 99-102.

11. Новикова Т.О., Сунгатов И.З. Модернизация и визуализация шифра Цезаря для повышения осведомленности в области защиты данных // Сб. научных статей 3-й Международной научно-технической конференции «Современное перспективное развитие науки, техники и технологий» - Воронеж: "Университетская книга", 2025. – С. 313-316.

12. Шарейко В. В. Использование программы с реализацией алгоритмов симметричного шифрования для олимпиадных заданий // В сб.: Информационные технологии в образовательном процессе вуза и школы. Материалы XIV Всероссийской научно-практической конференции. – Воронеж: ВГПУ, 2020. - С. 384-388.

13. К вопросу о способах дешифрования классических шифров / Марков Я.А. // Сб. трудов Двенадцатой международной научно-технической конференции «Безопасные информационные технологии». Москва, 2023. С. 165-169.

14. Wadik69, В. Дешифровка текста методом частотного анализа. / В. Wadik69 // Криптография. Шифрование и криптоанализ, 2020. - [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/513926/

15. Марков Я.А. Разработки эвристического способа анализа стойкости классических шифров. // Сб. трудов «80-е Дни науки Университета МИСИС». / Под общ. ред. М.Н.Давыдкина, - М.: НИТУ МИСИС, 2025. – Школьная секция - С. 1783-1784. – ISBN 978-5-907833-66-1.