МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Криптоанализ симметричных систем шифрования

АВТОРЕФЕРАТ
дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Власовой Софии Сергеевны

Научный руководитель
доцент, к. ф.-м. н. _____ А. В. Жаркова
23.01.2020 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2020 г.

Саратов 2020

ВВЕДЕНИЕ

Современная криптология – соревнование методов криптографии и криптоанализа. Фундаментальный принцип криптоанализа, впервые сформулированный Огюстом Керкхофсом, состоит в том, что секретность сообщения всецело зависит от ключа, то есть весь механизм шифрования, кроме значения ключа, известен противнику. Криптоанализ ставит своей задачей в разных условиях получить дополнительные сведения о ключе шифрования, чтобы значительно уменьшить диапазон вероятных ключей.

Повсеместно государственные стандарты шифрования данных основаны на симметричных блочных алгоритмах (например, ГОСТ Р 34.12–2015 в России и AES в США). Соответственно, методы криптоанализа подобных шифров позволяют выявлять уязвимости многих используемых и находящихся в разработке алгоритмов шифрования [1].

Основными методами криптоанализа блочных шифров считаются дифференциальный и линейный. С 1997 года также известен метод интегрального криптоанализа, впервые примененный Ларсом Кнудсеном. Для поточных шифров основными классами атак являются силовые, статистические и аналитические атаки.

Целью данной работы является изучение методов криптоанализа симметричных систем шифрования, в результате чего требуется разработать и реализовать программу для криптоанализа симметричного шифра одним из рассмотренных методов.

Для достижения поставленной цели требуется решить следующие задачи:

1) изучить различные методы криптоанализа симметричных систем шифрования;

2) выбрать алгоритм шифрования для программной реализации одного из методов криптоанализа;

3) разработать и реализовать программный продукт, позволяющий провести криптоанализ.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 89 страниц, из них 63 страницы – основное содержание, включая 27 рисунков и 3 таблицы, список использованных источников из 28 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе описаны основные определения согласно [1–9], которые используются в данной работе.

Во втором разделе описаны свойства симметричных шифров [10], общее строение блочных шифров [7] и методы криптоанализа блочных шифров.

В подразделе 2.1 вводятся понятия дифференциального криптоанализа [11], характеристик [12] и их свойств [15], описывается дифференциальный криптоанализ шифра DES согласно [14–15], описание шифра приведено в [13]. Существуют различные модификации метода дифференциального криптоанализа, эти модификации и сопутствующие им теоремы описаны в [12], [16–19].

В подразделе 2.2 приведено описание метода линейного криптоанализа, определение линейных аппроксимаций и примеры вычисления линейных аппроксимаций для разных вариантов шифра DES [20]. Вероятность выполнения полученного выражения подсчитывается с помощью леммы о набегании знаков [21].

В подразделе 2.3 приведено описание метода интегрального криптоанализа [22] и теоремы, доказывающей корректность этого метода [23].

Для практической реализации был выбран линейный метод криптоанализа, как наиболее эффективный алгоритм криптоанализа шифра DES.

Третий раздел посвящен методам криптоанализа поточных систем шифрования. Приведено общее описание поточных систем шифрования, дана классификация методов атак на поточные шифры, упомянута возможность применения методов дифференциального [24] и линейного [25] методов криптоанализа на поточные шифры. Подраздел 3.1 посвящен описанию аналитических методов криптоанализа поточных шифров, как самых часто используемых для криптоанализа данного вида шифров [26–27].

Четвертый раздел посвящен описанию программной реализации криптоанализатора шифра DES. В результате проделанной работы была

разработана и реализована программа на языке Python 3. Данная программа обладает следующим функционалом:

1) шифрование и расшифрование файлов с помощью алгоритмов DES3, DES5, DES8, DES10 и DES12;

2) генерация текстового файла. Пользователь может воспользоваться данной функцией, если у него нет достаточного объема данных для криптоанализа;

3) вычисление ключей шифров алгоритмов DES3, DES5, DES8, DES10 и DES12 методом линейного криптоанализа.

Листинг программы приведен в приложении А.

Для корректной работы программы также был создан файл config.py, в котором находятся *S*-блоки и таблицы перестановок, использующиеся в шифре DES. Листинг файла приведен в приложении Б.

В разделе представлены интерфейс программы и подробное описание ее работы с примерами реакции программы на самые ожидаемые ошибки пользователя, такие как некорректный размер ключа или невыбранный файл. Приведены пример работы программы с файлами формата .txt и .exe, а также в виде таблиц показаны статистические данные, собранные в ходе тестирования программы. Из этих таблиц видно, что основными критериями, определяющим время работы приложения, являются размер файла и выбранный алгоритм шифрования/расшифрования. Также в работе упомянут уже существующий программный продукт с похожим функционалом [28].

ЗАКЛЮЧЕНИЕ

В теоретической части данной работы были приведены общие сведения о блочных шифрах, а также рассмотрены различные методы криптоанализа этого типа шифров, такие как линейный, дифференциальный и интегральный, а также методы, основанные на этих основных методах. Также были рассмотрены аналитические методы криптоанализа поточных шифров. Были показаны их принципы функционирования, изучены достоинства и недостатки.

В результате проделанной теоретической работы было принято решение разработать и реализовать программу для криптоанализа блочных шифров DES3, DES5, DES8, DES10 и DES12, которые являются вариантами шифра DES.

Разработанная программа позволяет шифровать и расшифровывать файлы с помощью указанных алгоритмов, генерировать текстовые файлы для использования их в процедуре криптоанализа и полностью или частично вычислять ключ, использующийся для операций шифрования и расшифрования с помощью одного из указанных алгоритмов DES, выводить в файл результаты своей работы. Вычисление производится на основе некоторого файла и соответствующего ему зашифрованного файла. Взлом шифра проводится с помощью метода линейного криптоанализа, если необходимо вычислить ключ частично, и сочетанием методов линейного криптоанализа и полного перебора для вычисления всего ключа.

По результатам тестирования практической части проекта на всех исследуемых примерах все функции программы работали корректно. После последовательного выполнения операций шифрования и расшифрования программа возвращает файл, идентичный исходному. Функция генерации файлов создает файлы достаточного размера для проведения эффективной операции криптоанализа. Для всех предложенных пар файлов функция криптоанализа выводит корректные результаты для выбранного шифра DES.

Программу, разработанную и реализованную в ходе данной работы, можно использовать для шифрования и расшифрования различных файлов вне

зависимости от их расширения. Кроме того, данная программа позволяет вычислять ключи, использованные для шифрования или расшифрования файлов с помощью указанных алгоритмов. Эти ключи могут быть вычислены полностью или частично, после чего пользователь может использовать полученные значения в своих целях. Кроме того, возможность частичного вычисления ключа позволяет проверить корректность реализованного алгоритма линейного криптоанализа быстрее, чем вычисление точного значения ключа.

Таким образом, поставленные задачи были решены, цель работы можно считать достигнутой.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Салий, В. Н. Криптографические методы и средства защиты информации [Электронный ресурс] : учеб. пособие / В. Н. Салий // Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского. – Саратов, 2017. – 43 с. – URL: https://www.sgu.ru/sites/default/files/textdocsfiles/2017/10/18/saliy_v.n._kriptograficheskie_metody_i_sredstva_zashchity_informacii.pdf (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. рус.

2 Мао, В. Современная криптография: теория и практика [Электронный ресурс] / В. Мао. – М. : Издательский дом «Вильямс», 2005. – 768 с. – Загл. с экрана. – Яз. рус.

3 Слеповичев, И. И. Генераторы псевдослучайных чисел [Электронный ресурс] : учеб. пособие / И. И. Слеповичев // Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского. – Саратов, 2016. – 117 с. – URL: https://www.sgu.ru/sites/default/files/textdocsfiles/2018/07/09/slepovichevi.i.generator psevdosluchaynyh_ chisel_2017.pdf (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. рус.

4 Ковтун, В. Ю. Введение в криптоанализ. Криптоанализ симметричных криптосистем: блочные шифры [Электронный ресурс] : учеб. пособие / В. Ю. Ковтун // NRJETIX [Электронный ресурс] : [сайт]. – URL: http://www.nrjetix.com /fileadmin/doc/publications/Lectures_security/Lecture4-1.pdf (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. рус.

5 Сушко, С. А. Практическая криптология. Лекция 10 [Электронный ресурс] : учеб. пособие / С. А. Сушко // Национальный технический университет «Днепровская политехника». – URL: http://bit.nmu.org.ua/ua/ student/metod/ cryptology/лекция 10.pdf (дата обращения: 15.12.2019). – Загл. с экрана. – Яз. рус.

6 Ростовцев, А. Г. Методы криптоанализа классических шифров [Электронный ресурс] / А. Г. Ростовцев, Н. В. Михайлова. – М. : Наука, 1995. – 208 с. – Загл. с экрана. – Яз. рус.

7 Бабенко, Л. К. Дифференциальный криптоанализ алгоритма ГОСТ 28147-89 [Электронный ресурс] : научная статья / Л. К. Бабенко, Е. А. Ищукова // Известия Южного федерального университета. Технические науки, 2011. – № 12 (125). – С. 120–130. – URL: http://izv-tn.tti.sfedu.ru/wp-content/uploads/2011/12/14.pdf (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. рус.

8 Молдовян, Н. А. Криптография: от примитивов к синтезу алгоритмов [Электронный ресурс] / Н. А. Молдовян, А. А. Молдовян, М. А. Еремеев. – СПб. : БХВ-Петербург, 2004. – 448 с. – Загл. с экрана. – Яз. рус.

9 Пестунов, А. И. О некоторых направлениях научных исследований в области криптоанализа симметричных алгоритмов [Электронный ресурс] : научная статья / А.И. Пестунов, А.А. Перов, Т.М. Пестунова // Вестник НГУЭУ, 2016. – № 3. – С. 280–298. – URL: https://cyberleninka.ru/article/n/o-nekotoryh-napravleniyah-nauchnyh-issledovaniy-v-oblasti-kriptoanaliza-simmetrichnyh-algoritmov/viewer (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. рус.

10 . Бабенко, Л. К. Особенности применения методов дифференциального и линейного криптоанализа к симметричным блочным шифрам [Электронный ресурс] : научная статья / Л. К. Бабенко, Е. А. Ищукова // Вопросы кибербезопасности, 2015. – № 2. – С. 11–19. – URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb_10_02.pdf (дата обращения: 20.10.2019). – Загл. с экрана. – Яз. рус.

11 Агибалов, Г. П. Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом [Электронный ресурс] : научная статья / Г. П. Агибалов // Прикладная дискретная математика, 2008. – № 1(1). – С. 34–42. URL: https://cyberleninka.ru/article/v/elementy-teorii-

differentsialnogo-kriptoanaliza-iterativnyh-blochnyh-shifrov-s-additivnym-raundovym-klyuchom (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. рус.

12 Панасенко, С. П. Алгоритмы шифрования. Специальный справочник [Электронный ресурс] / С. П. Панасенко. – СПб. : БХВ-Петербург, 2009. – 576 с. – Загл. с экрана. – Яз. рус.

13 Сушко, С. А. Практическая криптология. Лекция 6 [Электронный ресурс]: учебное пособие / С. А. Сушко // Национальный технический университет «Днепровская политехника». – URL: http://bit.nmu.org.ua/ua/student/metod/cryptology/лекция 6.pdf (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. рус.

14 Biham, E. Differential cryptanalysis of DES-like cryptosystems [Электронный ресурс] : научная статья / E. Biham, A. Shamir // Journual of Cryptology, 1991. – №4 (1). – С. 3–72. URL: https://link.springer.com/article/10.1007/BF00630563 (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. англ.

15 Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Электронный ресурс] / Б. Шнайер. – М. : Диалектика, 2003. – 610 с. – Загл. с экрана. – Яз. рус.

16 Khurana, M. Variants of Differential and Linear Cryptanalysis [Электронный ресурс] : научная статья / M. Khurana, M. Kumari // International Journal of Computer Applications, 2015. – № 18. – С. 473–483. – URL: https://pdfs.semanticscholar.org/3354/37c4a046ea5bff7a1c408c9445232eabfc6e.pdf (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. англ.

17 Lai, X. Higher order differential cryptanalysis framework and its applications [Электронный ресурс] : научная статья / M. Duan, X. Lai // International Conference on Information Science and Technology, 2011. – С. 291–297. – URL: https://ieeexplore.ieee.org/abstract/document/5765256 (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. англ.

18 Секей, Г. Парадоксы в теории вероятностей и математической статистике [Электронный ресурс] : научная статья / Г. Секей. – М. : Мир, 1990. – 240 с. – Загл. с экрана. – Яз. рус.

19 Schneier, B. Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER and Triple-DES [Электронный ресурс] : научная статья / J Kelsey, B. Schneier, D. Wagner // CRYPTO 1996: Advances in Cryptology. – CRYPTO '96, 1996. – С. 237–251. – URL: https://link.springer.com/chapter/10.1007/3-540-68697-5_19 (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. англ.

20 Matsui, M. Linear Cryptanalysis Method for DES Cipher [Электронный ресурс] : научная статья / M. Matsui // EUROCRYPT 1993: Advances in Cryptology. – EUROCRYPT '93, 1993. – С. 386–397. URL: https://link.springer.com/chapter/ 10.1007/3-540-48285-7_33 (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. англ.

21 Kukorelly, Z. The Piling-Up Lemma and Dependent Random Variables [Электронный ресурс] : научная статья / Z. Kukorelly // IMA International Conference on Cryptography and Coding, LNCS, 1999. – Vol. 1746. – С. 186–190. – URL: https://link.springer.com/chapter/10.1007/3–540–46665–7_22 (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. англ.

22 Herstein, I. N. Topics in Algebra. [Электронный ресурс] / I. N. Herstein. – Chicago : John Wiley & Sons, 1975. – 400 с. – URL: https://marinazahara22.files.wordpress.com/2013/10/i-n-herstein-topics-in-algebra-2nd-edition-1975-wiley-international-editions-john-wiley-and-sons-wie-1975.pdf (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. англ.

23 Knudsen, L. Integral Cryptanalysis [Электронный ресурс] / L. Knudsen, D. Wagner // Proceedings of Fast Software Encryption FSE'02, 2002. – Vol. 2365. – С. 112–127. – URL: https://www.cosic.esat.kuleuven.be/nessie/reports/phase2/uibwp5-015-1.pdf (дата обращения: 26.09.2019). – Загл. с экрана. – Яз. англ.

24 Бабенко, Л. К. Дифференциальный криптоанализ поточных шифров [Электронный ресурс] : научная статья / Л. К. Бабенко, Е. А. Ищукова // Известия Южного федерального университета. Технические науки. – 2009. – Т. 100. – №. 11. – С. 232–238. – URL: https://cyberleninka.ru/article/n/differentsialnyy-kriptoanaliz-potochnyh-shifrov/viewer (дата обращения: 15.12.2019). – Загл. с экрана. – Яз. рус.

25 Golić, J. D. Linear cryptanalysis of stream ciphers [Электронный ресурс] : научная статья / J. D. Golić // International Workshop on Fast Software Encryption. – Springer, Berlin, Heidelberg, 1994. – С. 154–169. – URL: https://link.springer.com/chapter/10.1007/3-540-60590-8_13 (дата обращения: 15.12.2019). – Загл. с экрана. – Яз. англ.

26 Абзалов, В. Ш. Анализ методов криптоанализа поточных шифров [Электронный ресурс] : научная статья / В. Ш. Абзалов // Молодежный научный форум: технические и математические науки. – 2016. – №. 9. – С. 6–11. – URL: https://nauchforum.ru/studconf/tech/xxxviii/12718 (дата обращения: 15.12.2019). – Загл. с экрана. – Яз. рус.

27 Потий, А. Исследование методов криптоанализа поточных шифров / А. Потий, Ю. Избенко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2003. – Вип. 6. – С. 34–49. URL: https://ela.kpi.ua/bitstream/123456789/12378/1/06_p34.pdf (дата обращения: 15.12.2019). – Загл. с экрана. – Яз. рус.

28 crack.sh [Электронный ресурс] // URL: https://crack.sh (дата обращения: 15.12.2019). – Загл. с экрана. – Яз. англ.