**Лекция 8.**  Задачи и принципы криптоанализа. Классификация криптоатак.

**Задачи и принципы криптоанализа**

Следует заметить сразу, что основная цель криптоанализа состоит не столько в получении скрываемой информации, а в оценке стойкости существующих и разрабатываемых криптосистем. Оценка стойкости криптосистем представляется в виде количества операций, необходимых для взлома криптосистемы или в виде времени, которое требуется для взлома.

Приведем основные принципы, которые были «выстраданы» криптологами [5,10]:

1. Принцип Керкхоффа. Только криптоаналитик может судить о криптостойкости системы.

2. Принцип Керкхоффа-Шеннона. Противник знает используемую криптосистему с точностью до ключевой информации.

3. Принцип Жеверже. Поверхностные усложнения криптосистемы могут быть иллюзорны, так как порождают ложные оценки ее криптостойкости.

4. При оценке криптостойкости необходимо учитывать возможные криптографические ошибки и другие нарушения дисциплины безопасности.

Из приведенных выше принципов следует, что основная задача криптоаналитика заключается в оценке ключевой информации, при условии, что сама используемая криптосистема известна. Алгоритм оценки ключевой информации называется **криптоатакой**. В зависимости от условий взаимодействия криптоаналитика с криптосистемой различают следующие основные типы криптоатак:

* криптоатака с использованием только криптограмм (А1);
* криптоатака с использованием открытых текстов и соответствующих им криптограмм (А2);
* криптоатака с использованием выбираемых криптоаналитиком открытых текстов и соответствующих им криптограмм (А3);
* криптоатака с использованием аппаратного воздействия на криптосистему (криптоатака по сторонним каналом) (А4).

Последний тип криптоатак А4 предполагает не исследования теоретического описания криптографического алгоритма, а анализ данных, полученных в результате наблюдения за физическим процессом работы устройства, реализующего криптографический алгоритм. К этому типу криптоатак относятся: криптоатака по времени, криптоатака по энергопотреблению, криптоатака по электромагнитному излучению, криптоатака на основе акустического анализа.

В настоящее время разработано множество методов криптоанализа, реализующих криптоатаки типов А1-А3. В настоящей главе рассмотрим несколько этих типов криптоатак.

**Классификация криптоатак**

**I. Атака с известным шифртекстом** (ciphertext only attack). Предполагается, что противник знает алгоритм шифрования, но не знает секретный ключ. Кроме того, в его распоряжении имеется набор перехваченных шифрограмм. Разновидности:

- **полный перебор ключей**;

- **атака по словарю**, перебор ключей по словарю (dictionary attack). Использование Интернет-червя в 1988 г. предоставляет хорошо документированный случай взлома паролей. Интернет-червь пытался взломать пароли, работая с серией словарей. На первом этапе атаки было использовано множество слов, содержащее имена пользователей, взятых из файла паролей системы Unix. Если это не имело успеха, использовался внутренний словарь 432 общепринятых, используемых в Интернет-жаргоне, слов. Если второй этап не имел успеха, использовался Unix словарь, состоящий из 24474 слов. Червь также проверял на пустой пароль. Сайты, на которые производилась атака, сообщили, что около 50 % паролей было успешно взломано, используя данную стратегию;

- **частотный криптоанализ** - метод вскрытия шифра, основывающийся на предположении о существовании зависимости между частотой появления символов в открытых сообщениях и соответствующих шифрозамен в шифрограммах. Метод частотного криптоанализа известен с IX-го века (работы Ал-Кинди), хотя наиболее известным случаем его применения в реальной жизни, возможно, является дешифровка египетских иероглифов Ж.-Ф. Шампольоном в 1822 г. В художественной литературе наиболее известными упоминаниями являются рассказы «Золотой жук» Эдгара По, «Пляшущие человечки» Конан Дойля, а также роман «Дети капитана Гранта» Жюль Верна.

**II. Атака с выбором шифртекста** (chosen ciphertext attack). Криптоаналитик имеет возможность выбрать необходимое количество криптограмм и получить соответствующие им открытые тексты. Криптоаналитик может воспользоваться устройством расшифрования один или несколько раз для получения шифротекста в расшифрованном виде. Используя полученные данные, он может попытаться восстановить секретный ключ для расшифровки.

**III. Адаптивная атака с выбором шифртекста** (adaptive chosen ciphertext attack). Криптоаналитик имеет возможность выбирать новые шифрограммы для расшифровки с учетом того, что ему известна некоторая информация из предыдущих сообщений. В некоторых криптографических протоколах при получении шифрограммы, несоответствующей стандарту (содержащей ошибки), отправитель получает ответное сообщение, иногда с детализированным описанием этапа проверки и причины возникновения ошибки. Криптоаналитик может использовать эту информацию для последовательной посылки и уточнения параметров криптосистемы.

**IV. Атака с известным открытым текстом** (known plaintext attack). То же, что и предыдущая, но противник для некоторых шифрограмм получает в свое распоряжение соответствующие им открытые сообщения. Во время «холодной войны» американские дипломаты в Москве пользовались шифровальными машинами, получившими кодовое название «бриллианты». Оборудование располагалось на девятом этаже здания посольства США в особо защищенном помещении, называвшемся узлом связи. Внутри этого помещения была еще одна комната, где шифровальные машины зашифровывали и расшифровывали шифрограммы, которыми обменивались посольство и штаб-квартира ЦРУ в Лэнгли (штат Виргиния). В другой части узла связи другие машины передавали перехваченную АНБ информацию или вели обмен сообщениями между Госдепартаментом и его представителями в Москве. Чтобы обеспечить как можно более полную защиту этого помещения, были предприняты особые меры безопасности в отношении его стен, электропроводки, линий электропитания и подачи воздуха. Сами шифровальные машины представляли собой новейшую разработку АНБ с цифровыми кодами на магнитных лентах, которые менялись каждые 24 часа. Кроме того, каждое сообщение пропускалось через две машины, зашифровываясь дважды. Все это создавало впечатление неуязвимости как узла связи, так и «бриллиантов». Но, несмотря на все меры безопасности, русские сумели тайно подменить «чистые» кабели электропитания шифровальных машин. Таким образом они смогли обойти электронные фильтры защиты и улавливали сигналы напрямую с «бриллиантов». В печатающих устройствах шифровальных машин были заменены печатные платы и кремниевые микросхемы, что позволило агентам КГБ снимать и записывать незашифрованные сигналы с линий связи и принтеров. Получив в свое распоряжение открытый текст, они имели возможность затем сравнить его с зашифрованными сообщениями и найти ключи шифрования.

**V. Атака с выбором открытого текста** (chosen plaintext attack). Криптоаналитик обладает определённым числом открытых текстов и соответствующих шифротекстов, кроме того, он имеет возможность зашифровать несколько предварительно выбранных открытых текстов (до начала атаки). Разновидности:

- **временный доступ к шифрующему устройству** - американским спецслужбам удалось, подкупив охрану, выкрасть из японского посольства шифровальную машину на два дня. Возможность взлома машины была исключена, так как это бы привело к раскрытию операции и к смене всех ключей. Зато, американцы получили возможность осуществить атаку японского шифра на основе подобранного открытого текста;

- **использование информации о структуре сообщений или стандартных фразах** – криптоаналитики из Блетчли-Парка могли определить открытый текст сообщений в зависимости от того, когда эти сообщения были посланы. Например, ежедневный отчет о погоде посылался немецкими связистами в одно и то же время. По той причине, что военные доклады имеют определенную структуру, криптоаналитикам удавалось расшифровывать остальную информацию, пользуясь данными о погоде в той местности. Другим ярким примером являлись перехваченные сообщения офицера африканского корпуса, который постоянно отсылал «Нечего докладывать». Другие операторы тоже часто использовали стандартные ответы или приветствия;

- **перебор ключей по словарю** (dictionary attack) – криптоаналитик шифрует слова и фразы, наличие которых предполагается в шифрограмме, с использованием различных ключей. Совпадение зашифрованных слов и фраз с частями шифрограммы может говорить об обнаружении ключа;

- **получение документа и** [**ЭЦП**](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema12) **к нему**, сгенерированной с помощью закрытого ключа.

**VI. Адаптивная атака с выбором открытого текста** (adaptive chosen plaintext attack). Криптоаналитик имеет возможность выбирать новые открытые тексты с учетом того, что ему известна некоторая информация из предыдущих сообщений. Т.е. он может получить пары «открытое сообщение – шифрограмма», в т.ч. и после начала атаки. Разновидности:

- **провоцирование противника на использование в сообщениях определенных слов или фраз** – во время Второй мировой в Блетчли-Парк был придуман следующий способ заставить немцев отсылать определенные сообщения. По просьбе криптоаналитиков Королевские военновоздушные силы Великобритании минировали определенные участки Северного моря, этот процесс был назван «Садоводством» (англ. «gardening»). Практически сразу после этого немцами посылались зашифрованные сообщения, включающие слово «мины» и названия мест, где они были сброшены;

- **дифференциальный криптоанализ** – метод вскрытия симметричных блочных шифров (и других криптографических примитивов, в частности, хеш-функций), основанный на изучении разностей между шифруемыми значениями на различных раундах для пары подобранных открытых сообщений при их шифровании с одним и тем же ключом. Предложен в 1990 г. израильскими специалистами Эли Бихамом и Ади Шамиром. Является статистической атакой, в результате работы которой предлагается список наиболее вероятных ключей шифрования. Дифференциальный криптоанализ применим для взлома [DES](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema7#p72), FEAL и некоторые других шифров, как правило, разработанных ранее начала 90-х. Количество раундов современных шифров (AES, Camellia и др.) рассчитывалось с учетом обеспечения стойкости, в т.ч. и к дифференциальному криптоанализу;

- **интегральный криптоанализ** – аналогичен дифференциальному криптоанализу, но в отличие от него рассматривает воздействие алгоритма не на пару, а сразу на множество открытых текстов. Впервые применен в 1997 г. Ларсом Кнудсеном;

- **линейный криптоанализ** – метод вскрытия шифра, использующий линейные приближения для описания его работы. Линейный криптоанализ был изобретён японским криптологом Мицуру Мацуи (Mitsuru Matsui). Предложенный им в 1993 г. алгоритм был изначально направлен на вскрытие [DES](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema7#p72) и FEAL. Впоследствии линейный криптоанализ был распространён и на другие алгоритмы. На сегодняшний день наряду с дифференциальным криптоанализом является одним из наиболее распространённых методов вскрытия блочных шифров. Разработаны атаки на блочные и потоковые шифры. Криптоанализ выполняется в два шага. Первый – построение линейных соотношений между открытым текстом, шифрограммой и ключом, которые справедливы с высокой вероятностью. Второй – использование этих соотношений вместе с известными парами «открытый текст – шифрограмма» для получения битов ключа;

- **использование открытых ключей в ассиметричных системах** – криптоаналитик имеет возможность получить шифротекст, соответствующий выбранному сообщению, на основе открытого ключа.

**VII. Атака на основе связанных ключей** (related key attack). Криптоаналитик знает не сами ключи, а некоторые различия (соотношения) между ними. Множество реальных систем используют разные ключи, связанные известным соотношением. Например, для каждого нового сообщения предыдущее значение ключа увеличивается на единицу.

**VIII. Атака с выбором ключа** (chosen key attack). Криптоаналитик задает часть ключа, а на оставшуюся часть ключа выполняет атаку на основе связанных ключей.