Реферат

на тему:

Криптоанализ «Энигмы»

Киев 2018

«Эни́гма» - это переносная роторная шифровальная машина, использовавшаяся для шифрования и расшифрования секретных сообщений. Более точно, «Энигма» — целое семейство электромеханических роторных машин, применявшихся с 20-х годов XX века.

«Энигма» использовалась в коммерческих целях, а также военными службами во многих странах мира, но наибольшее распространение получила в нацистской Германии во время Второй мировой войны. Как мы знаем, именно эта машина использовалась для шифрования и расшифровывания сообщений, но мало кто знает как она работает, а тем более как удалось её взломать. Впервые шифровальные роторные машины начали использоваться в начале 20 века. Основным компонентом таких устройств является диск (он же ротор) с 26 электрическими контактами на обоих сторонах диска. Каждый контакт соответствовал букве английского алфавита. Соединение контактов левой и правой сторон реализовывало шифр простой замены. При вращении диска контакты смещались, изменяя тем самым подстановку для каждой буквы. Один диск обеспечивал 26 различных подстановок. Это означает, что при шифровании одного и того же символа, получаемая в результате последовательность начинает повторяться через 26 шагов.
Для увеличения периода последовательности можно использовать несколько роторов, соединенных последовательно. При совершении полного оборота одного из дисков, следующий диск сдвигается на одну позицию. Это увеличивает длину последовательности до 26^n, где n — количество соединенных последовательно роторов.

Чем же отличалась «Энигма»? Она является наиболее популярным представителем мира шифровальных роторных машин и считалась практически не взламываемой.

Число роторов в разных версиях «Энигмы» могло отличаться. Наиболее распространенной была «Энигма» с тремя роторами, но использовался так же вариант с четырьмя дисками. Также процесс расшифровки отличался от процесса шифрования. Каждый раз для расшифровки пришлось бы менять левый и правый ротор местами, что может быть не совсем удобным. Для решения этой проблемы в «Энигме» был добавлен еще один диск, который назывался рефлектор. В рефлекторе все контакты были соединены попарно, реализуя тем самым повторное прохождение сигнала через роторы, но уже по другому маршруту. В отличие от остальных роторов рефлектор всегда находился в фиксированном положении и не вращался.

Еще одно свойство Энигмы, связанное с рефлектором, заключается в невозможности шифрования какой-либо буквы в саму себя. Это свойство сыграло очень важную роль при взломе Энигмы.

Стойкость подобной машины упирается в секретность внутренней коммутации роторов. Если устройство роторов будет раскрыто, то взлом сводится к подбору их начальных позиций.

Так как каждый ротор может находится в одной из 26 позиций, для трех роторов получаем 26^3=17476 вариантов. При этом сами роторы тоже могут располагаться в произвольном порядке, что увеличивает сложность в 3! раз. Т.е. пространство ключей такой машины составит 6*17576=105456. Этого было недостаточно для того, чтобы обеспечить высокий уровень безопасности. Поэтому Энигма было оснащена еще одним дополнительным инструментом: коммутационной панелью. Она позволяла любому оператору усложнять шифр за счет варьирования соединения проводов еще до прохождения сигнала через роторную часть. Энигму с коммутационной панелью было гораздо сложнее «взломать», поскольку невозможно было математически объяснить принцип замены букв. Соединяя на коммутационной панели буквы попарно можно было добавить еще один дополнительный шаг к шифрованию.

Считалось, что благодаря столь сложному устройству Энигму невозможно взломать, поэтому французская и британская разведки верили, что расшифровать сообщения нацистов можно, лишь выкрав одну из машин и внедрив в немецкую армию спецагента, который будет информировать союзников о ежедневно меняющихся настройках Энигмы. Этот план был недолговечен. Исчезновение любой из машин Энигма сразу бы заметили, и машину немедленно переделали.

После того как мы наконец разобрались с устройством машины, я хотел бы рассказать про сам криптоанализ.

Первые попытки взломать код «Энигмы» предприняли польские дешифровщики. В межвоенный период там сформировалась сильная группа математиков-криптоаналитиков. Они взломали шифр Красной Армии во время советско-польской войны 1919-1921 гг. и тем самым предопределили ее поражение. В 1939 году они перебрались во Францию, а затем в Великобританию. Ими была переданы образцы машины и разработки по ее дешифровке. В Англии работа была сосредоточена в GC&CS — Government Code and Cypher School — Правительственная школа кодов и шифров. Так началась операция «Ультра». Она поставляла огромный объем информации высшей категории секретности из Германии и Италии для высших английских руководителей, а потом и для командующих союзными войсками в Европе.

Главную роль в дешифровке шифров не только «Энигмы», но и других немецких шифровальных машин сыграл выдающийся математик Алан Тьюринг. В середине 1930 гг. он создал математическую модель, на основе которой строятся все компьютеры (машина Тьюринга). Именно он разработал главные алгоритмы дешифровки и теоретические основы создания компьютера Colossus (Колосс). С введением его в строй время расшифровки сообщений сократилось до нескольких часов. Он считается первым программируемым компьютером в истории вычислительной техники.

Свою роль во взломе «Энигмы» сыграли метеопрогнозы. Немцы методично начинали их с одного и того же слова, а заканчивали восхвалением Гитлера. Зная, откуда пришел метеопрогноз и какая была погода, можно было составить представление о характере открытого текста. Помогала и особенность грамматики немецкого языка, а также захваты шифровальных книг на немецких кораблях и подводных лодках. Важнейшей была задача не допустить, чтобы немцы, а потом и японцы догадались о взломе шифровальной машины. Для этого предпринимались самые разные действия.

Перехват радиосообщений противника выполняли десятки приемных станций, имевших кодовое название «Y-station». Ежедневно в Блетчли-парк поступали тысячи таких сообщений. Блетчли-парк имел в своем распоряжении точную копию «Энигмы», поэтому расшифровка сообщений сводилась к подбору установки дисков и, для более поздних моделей, — штекерного коммутатора. Сложность задачи усугублялась тем, что установки роторов менялись ежедневно, поэтому службы дешифровки работали круглосуточно в три смены.

Конструкция «Энигмы» при правильном использовании обеспечивала практически полную секретность. На практике, однако, со стороны немецких пользователей «Энигмы» зачастую допускались небрежные действия, дававшие подсказки британским аналитикам. Именно на использовании и систематизации таких погрешностей и был основан метод дешифровки.

Подсказками служили любые часто повторяющиеся тексты, такие как приветствия, цифры (кодировались по произношению: «один», «два» и т. д). Все подсказки заносились в картотеку (Index) вместе с контекстом: почерком радиста, местом и временем передачи и т. п.

При отсутствии необходимого количества подсказок, особенно накануне крупных операций, проводились специальные мероприятия по их получению. Этот прием получил кодовое название «садоводство». Например, перед выходом очередного полярного конвоя проводилось демонстративное минирование определённого участка моря. Если противник докладывал результаты разминирования с указанием заранее известных координат, это давало искомую подсказку.

В августе 1940 года была построена криптоаналитическая машина *Bombe*. Со временем в Блетчли-Парке было установлено более 200 машин, что позволило довести темп расшифровки до двух-трёх тысяч сообщений в день.

Абсолютная надежность не вызывала никаких сомнений у немецких специалистов: до самого конца войны немецкое командование искало причины утечек секретной информации где угодно, но не в раскрытии «Энигмы». Именно поэтому успех британских дешифровщиков стал особенно ценным вкладом в дело победы над нацизмом.

Источники:

1)https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7_%C2%AB%D0%AD%D0%BD%D0%B8%D0%B3%D0%BC%D1%8B%C2%BB#cite_note-22

2)https://uk.wikipedia.org/wiki/%D0%95%D0%BD%D1%96%D0%B3%D0%BC%D0%B0_(%D0%B0%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82)

3) https://habr.com/post/269519/

4) https://politeka.net/reading/analytics/450761-vtoraya-mirovaya-vojna-shifrov-vzlom-enigmy-i-srazheniya-matematikov/