Исследователь из Норвегии по имени Кристофер Кох 2009 году купил биткоинов на сумму 27 долларов и забыл про них, а когда вспомнил, его инвестиция подорожала до 887 тысяч долларов, а покупал он те биткоины для своей дипломной работы по криптографии.

Таким образом, биткоин — это электронная валюта нового поколения, созданная по подобию золота и обеспечивающая достаточный уровень надежности и безопасности.

ЛИТЕРАТУРА

1. Bitcoin – что это такое? [Электронный ресурс] / Great-World.ru. – 2017. / Режим доступа: http://great-world.ru/bitcoin-chto-eto-zarabotat. – Дата доступа 01.04.2017.

2. Удивительные факты о "криптовалюте" Bitcoin [Электронный ресурс] / HiTech.ru. – 2017. / Режим доступа: http://hitech.vesti.ru/news/view/id/3771/ Дата доступа: 01.04.2017.

Студ. Н. Н. Чобот

Науч. рук. проф., д. т. н. П. П. Урбанович
(кафедра информационных система и технологий, БГТУ)

АЛАН ТЬЮРИНГ И ЕГО СИСТЕМА ВЗЛОМА МАШИНЫ «ЭНИГМА»

Алан Тьюринг — математик, логик, криптограф. Знаменит исследованиями в области вычислимости, занимался расшифровкой машины «Энигмы». Тьюринг является одним из основоположников информатики [1].

Во время Второй мировой войны Тьюринг работал в Блетчли-парке — британском криптографическом центре, где возглавлял одну из 5 групп, Hut 8, занимавшихся в рамках проекта «Ультра» расшифровкой закодированных немецкой шифровальной машиной «Энигма» сообщений. Историк и ветеран Блетчли-парка однажды сказал: «Блетчли-парку был нужен исключительный талант, исключительная гениальность, и гениальность Тьюринга была именно такой».

Польские коллеги накануне Второй мировой войны пытались пробить брешь в кодировке и создать «свою криптологическую бомбу», используя ошибки немецких шифровальщиков, пробуя

полный перебор всех возможных комбинаций, что требовало просто нереальных затрат сил и времени. Но тогда немцы, узнав это, усовершенствовали «Энигму», сделав её еще сложнее. В начале 1940 года Алан Тьюринг, основываясь на разработках поляков, предложил *более эффективный и наиболее общий способ*: перебор последовательностей символов на основе подобранного открытого текста. Достаточно было ежедневно узнавать или угадывать один небольшой отрывок из сообщения. Это было не сложно, так как немецкие военные общались между собой достаточно стереотипными фразами. Далее механическим перебором двадцати шести символов латинского алфавита было нетрудно определить точное место этого отрывка в полном зашифрованном тексте. Перебор ключей выполнялся за счёт вращения механических барабанов, сопровождавшегося звуком, похожим на тиканье часов, из-за чего «Бомба» и получила своё название. Для каждого возможного значения ключа, заданного положениями роторов (количество ключей равнялось примерно 10^{19} для сухопутной «Энигмы» и 10^{22} для шифровальных машин, используемых в подводных лодках), «Бомба» выполняла сверку с известным открытым текстом, выполнявшуюся автоматически.

TuringBombe — электронно-механическая машина для расшифровки кода «Энигмы». Главной целью этого изобретения было нахождение ежедневных настроек машины «Энигма» на различных немецких военных соединениях: в частности, позиции роторов. Позиции роторов определяют ключ зашифрованного сообщения.

Первая Bombe была запущена 18 марта 1940 года. Дизайн «Бомб» Тьюринга также был основан на дизайне одноимённой машины Реевского. Машина TuringBombe состояла из 108 вращающихся электромагнитных барабанов и ряда других вспомогательных блоков. Она была 3,0 м длиной, 2,1 м высотой, 0,61 м шириной и весила 2,5 тонны. Серийно выпускалась до сентября 1944 года, когда ход войны сделал ненужным увеличение их количества.

Всего в «Блетчли-Парке» было установлено 210 машин типа Bombe, что позволило ежедневно расшифровывать до 3 тысяч сообщений. Это внесло существенный вклад в военные усилия Британии, в особенности в борьбу с подводными лодками в Атлантике. В числе полученной информации были и сведения о подготовке вторжения в СССР.

Принцип работы «криптологической бомбы». Расшифровать сообщения немецкой машины «Энигма» возможно лишь в том случае, если известен ключ, то есть положение роторов. Для того, чтобы его узнать, «Бомба» повторяет действия нескольких соединённых вместе машин «Энигма». Стандартная «Энигма» имеет три ротора, каждый из которых может быть установлен в любую из 26 позиций. Машина «Бомба» есть эквивалент 26 машинам «Энигма», каждая из которых состоит из трёх барабанов. «Бомба» может одновременно работать над тремя ключами секретных сообщений. В отличие от роторов «Энигмы», машина «Бомба» имеет барабаны с входными и выходными контактами. Таким образом, они могут быть соединены последовательно. Каждый барабан имел 104 проволочные щётки, которые касались пластин, на которые они были загружены. Щётки и соответствующий набор контактов на пластине были организованы в четырёх концентрических кругах из 26. Внешняя пара кругов была эквивалентна току, проходящему через «Энигму» в одном направлении, в то время как внутренняя пара была эквивалентом тока, проходящего в противоположном направлении.

Пример разгадывания исходного сообщения. Прогноз погоды всегда начинался со слов: WETTERVORHERSAGEBISKAYA

Допустим, что шифротекст выглядит таким образом: …QFZWRWIVTYRESXBFOGKUHQBAISEZ…

Для того, чтобы узнать соответствие букв, необходимо сопоставить эти тексты таким образом, чтобы буква не шифровалась сама в себя:

Q F Z W R W I V T Y R E ***S*** X B F O G K U H Q B A I S E Z

W E T T E R V O R H E R ***S*** A G E B I S K A Y A

Буква S шифруется сама в себя:

Q F Z W R W I V T Y R E S X B F O G K U H Q B A I S E Z
W E T T E R V O R H E R S A G E B I S K A Y A

Таким образом, если тексты правильно сопоставлены, то получается, что R расшифровывается как W на первой позиции и так далее:

R W I V T Y R E S X B F O G K U H Q B A I S E
W E T T E R V O R H E R S A G E B I S K A Y A

Вывод. Машина, созданная на основе этой спецификации, выполняла следующие последовательные действия:

1. Искала возможные настройки, использованные для шифрования сообщений (порядок роторов, положение ротора, соединения коммутационной панели), опираясь на известный открытый текст.

2. Для каждой возможной настройки ротора (у которого было 10^{19} состояний или 10^{22} в модификации, использовавшейся на подводных лодках) машина производила ряд логических предположений, основываясь на открытом тексте (его содержании и структуре).

3. Определяла противоречие, отбрасывала набор параметров и переходила к следующему. Таким образом, бóльшая часть возможных наборов отсеивалась и для тщательного анализа оставалось всего несколько вариантов.

А.Тьюринг занимался также разработкой шифров для переписки Черчилля и Рузвельта, проведя период с ноября 1942 года по март 1943 года в США.

ЛИТЕРАТУРА

1 Свободная энциклопедия «Википедия» [Электронный ресурс] / Тьюринг, Алан. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%A2%D1%8C%D1%8E%D1%80%D0%B8%D0%BD%D0%B3,_%D0%90%D0%BB%D0%B0%D0%BD. — Дата доступа: 01.04.2017