Санкт-Петербургский Национальный Исследовательский Университет ИТМО

Факультет программной инженерии и компьютерной техники

Сравнительный анализ технологий античности и современных аналогов

Выполнил:

Студент группы P3117

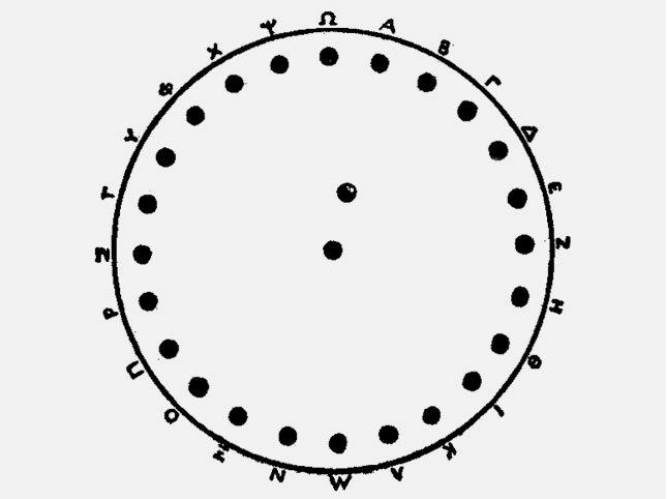
Пономарёв М. И.

Преподаватель:

Васильев А. В.

Санкт-Петербург
2022

Криптографический диск Энея
(Aeneas' cryptographic disc)



Древнегреческий полководец Эней Тактик в IV веке до н. э. предложил устройство, названное впоследствии «диском Энея». Это устройство представляло из себя глиняный диск диаметром 10-15 см и толщиной 1-2 см. На нём высверливались отверстия, каждое из которых соответствовало некоторой букве алфавита.

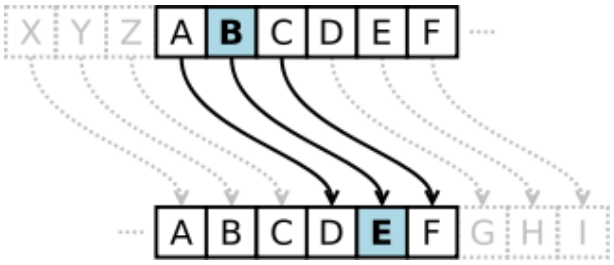
Принцип его работы был устроен следующим образом:

В центре диска помещалась катушка с нитками, при шифровании сообщения нитки последовательно протягивались через отверстия, создавая набор слов.

Чтобы расшифровать послание, получателю необходимо было последовательно вытягивать катушку в обратном порядке, таким образом получая сообщение в обратном порядке следования букв.

При перехвате диска недоброжелатель имел возможность таким же способом прочитать сообщение, что и получатель. Однако Эней предусмотрел возможность уничтожения передаваемого сообщения при угрозе захвата диска. Для этого было достаточно выдернуть катушку с нитками до полного их выхода из отверстий.

Современные криптографические методы



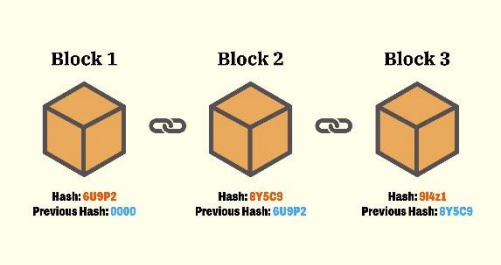
Криптографический диск Энея является одним из первых криптографических устройств, которое положило начало криптографии как науке. Наряду с диском, Эней придумал и другие способы передачи секретной информации, использующие тот же механизм шифрования.

Криптографический диск Энея является одним из первых шифров подстановки. После него стали известны такие методы шифрования как “шифр Цезаря”, также похожий подход был использован в криптографической машине “Энигма”.

Шифр Цезаря, также известный как шифр сдвига, на данный момент один из самых простых и широко известных методов шифрования. Его метод заключается в том, что каждый символ в тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите.

Энигма представляла из себя переносную шифровальную машину, использовавшуюся для шифрования и расшифрования секретных сообщений. Первую версию роторной шифровальной машины запатентовал в 1918 году Артур Шербиус.

Данное устройство состояло из определенного количества дисков, нанизанных на единую ось. Каждый из них делился на 26 частей, каждая из которых обозначало букву. Буквы на дисках были расставлены в случайном порядке. Оператор путем вращения дисков набирал нужное сообщение, а затем переписывал другую строчку. Человек, принявший данное сообщение, должен был обладать точно таким же устройством с точно такой же расстановкой букв.



Следующим прорывом в развитии криптографии стало создание криптографии на открытых ключах в 1970 годах, которая используется до сих пор в таких технологиях как “Blockchain”, “SSL”, “TLS”, “SSH” и других.

Сравнение античной и современной технологии

Затраты ресурсов:

Для изготовления диска Энея не требуется сложных и дорогих материалов, в чем оно имеет огромное преимущество перед настоящими шифровальными устройствами и компьютерами.

Эффективность:

Диск Энея очень прост и был достаточно эффективен в 14 веке, однако в настоящее время данный метод шифрования является неактуальным и чрезмерно примитивным. Настоящие методы шифрования являются гораздо совершеннее, надёжнее и используются повсеместно для безопасной отправки паролей по сетям при совершении покупок по интернету, для сохранения паролей пользователей в банковских и почтовых системах.

Используемое инженерное решение:

Инженерное решение в технологии диска Энея заключается в том, чтобы сделать диск с отверстиями по его периметру для того, чтобы было быстро и удобно составить шифр.

Инженерное решение в современных криптографических машинах состоит в неизмеримом множестве ключей для шифрования, что делает шифр практически

“невзламываемым”.