Криптография: история развития и базовые знания

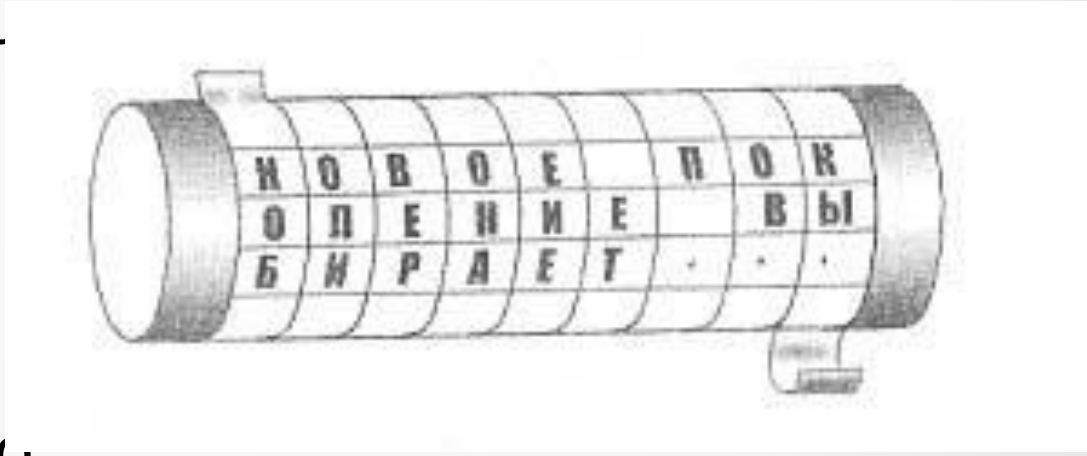
- «Новая большая игра — это отнюдь не война за нефтепроводы... Новое всемирное сокровище — это контроль над гигантскими потоками данных, соединяющими целые континенты и цивилизации, связывающими в единое целое коммуникацию миллиардов людей и организаций»

Наука криптография

- Криптогра́фия (от др.-греч. κρυπτός — скрытый и γράφω — пишу) - наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта)
- Эней Тактик (IV век до н. э.) - описание «книжного шифра» — метода передачи секретных сообщений с помощью малозаметных пометок рядом с буквами в книге или документе

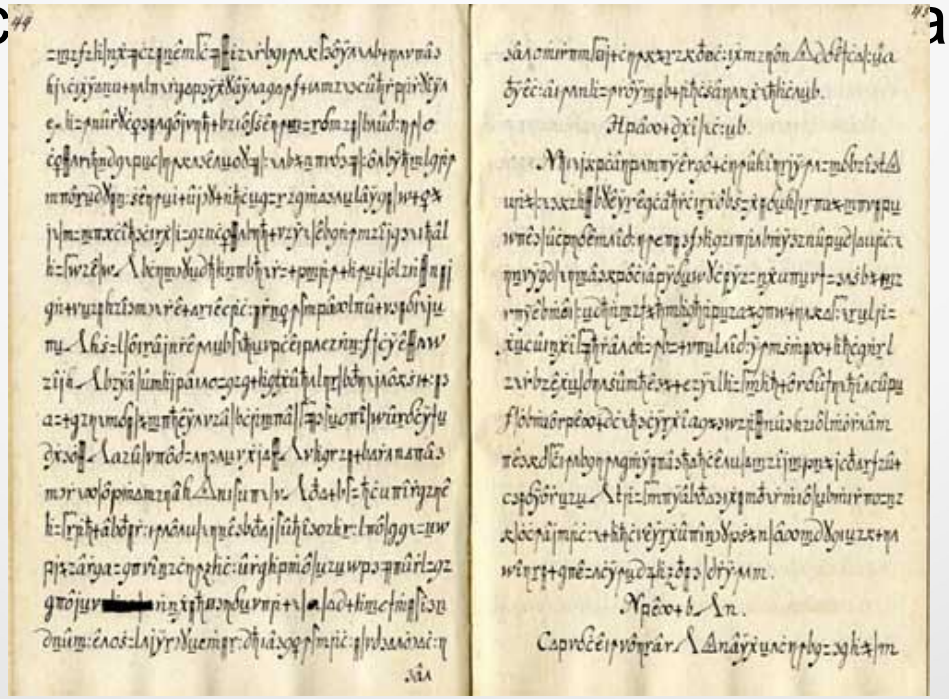
Спарта

- Писцы Древнего Египта часто использовали изощренные способы письма, чтобы привлеч внимание к своим текстам. Чаще всего шифровка информаци использовалась в военных целях: широко известен шифр «Скитала», примененный Спартой против Афин в V веке до н. э.

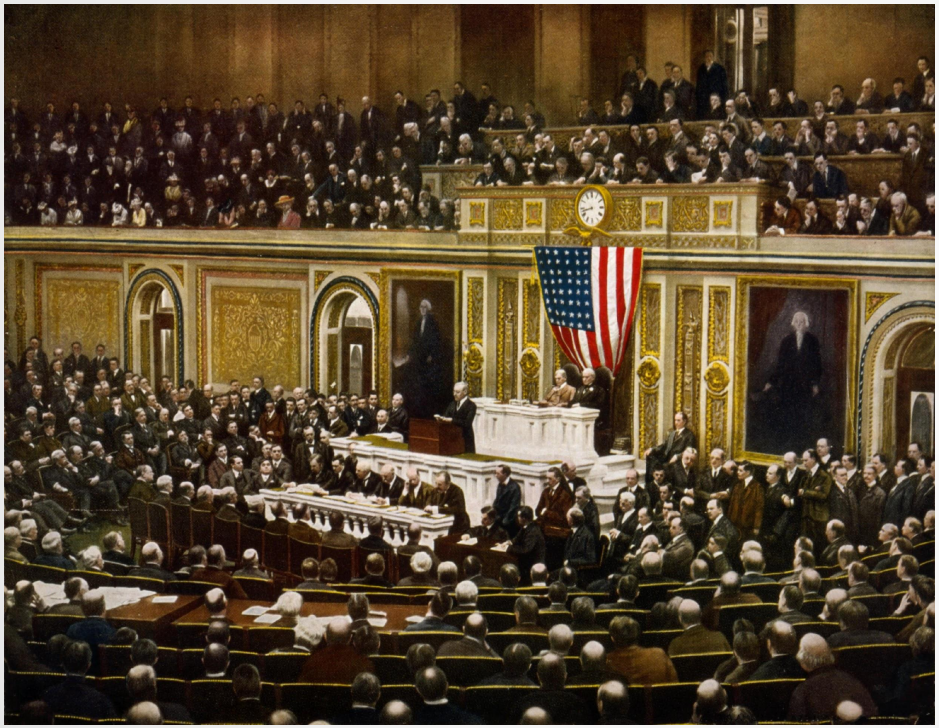


Средние века

- Одним из самых известных шифров Средних веков называют кодекс Copiale — изящно оформленную рукопись с водяными знаками, не расшифрованную до сих пор. Эпоха Возрождения стала золотым веком криптографии: ее изучением занимался Фрэнсис Бэкон, описавший с а.



Первая мировая война



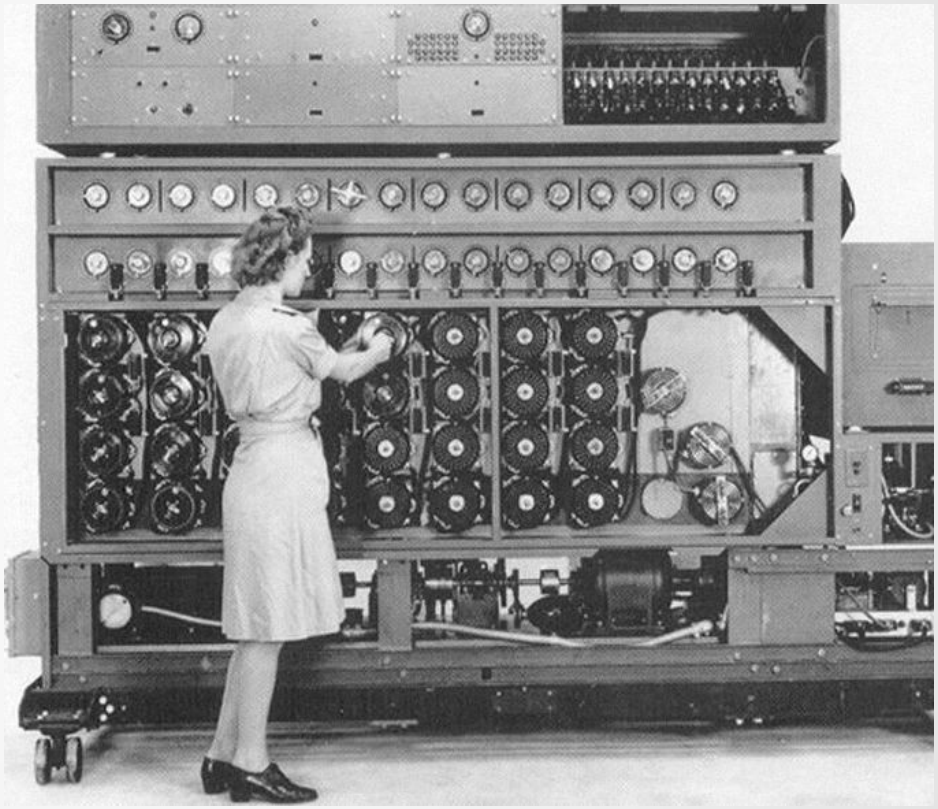
- Во время Первой мировой войны криптография стала признанным боевым инструментом. Разгаданные сообщения противников вели к ошеломляющим результатам. Перехват телеграммы немецкого посла Артура Циммермана американскими спецслужбами привел к

Вторая мировая война

- Использованные шифровальные машины (немецкая «Энигма», английская «Бомба Тьюринга») ясно показали жизненную важность информационного контроля. В послевоенное время правительства многих стран наложили мораторий на использование криптографии

.«Энигма»

- Разработанный под руководством Алана Тьюринга дешифратор. Его использование позволило союзникам расколоть казавшийся монолитным код «Энигмы».



Современные методы использования криптографии

- Появление доступного интернета перевело криптографию на новый уровень. Криптографические методы стали широко использоваться частными лицами в электронных коммерческих операциях, телекоммуникациях и многих других средах. Первая получила особенную популярность

Разведка

- Номерны́е радиоста́нции — коротковолновые радиостанции, о принадлежности которых достоверно не известно. Они передают в эфир набор чисел, слов или букв, который зачитывает диктор или компьютер. В некоторых случаях используется фонетический алфавит. Передаваемые данные представляют собой

Терминологияя

Криптоанализ — наука, изучающая математические методы нарушения конфиденциальности и целостности информации.
Криптография и криптоанализ составляют криптологию, как единую науку о создании и взломе шифров (такое деление привнесено с запада, до этого в СССР и России не применялось специального деления).
Криптографическая стойкость — способность криптографического алгоритма противостоять криптоанализу.
Криптографическая атака — попытка криптоаналитика вызвать отклонения в атакуемой защищённой системе обмена информацией. Успешную криптографическую атаку называют взлом или вскрытие.

Спасибо за внимание!