История криптографии

Криптография?

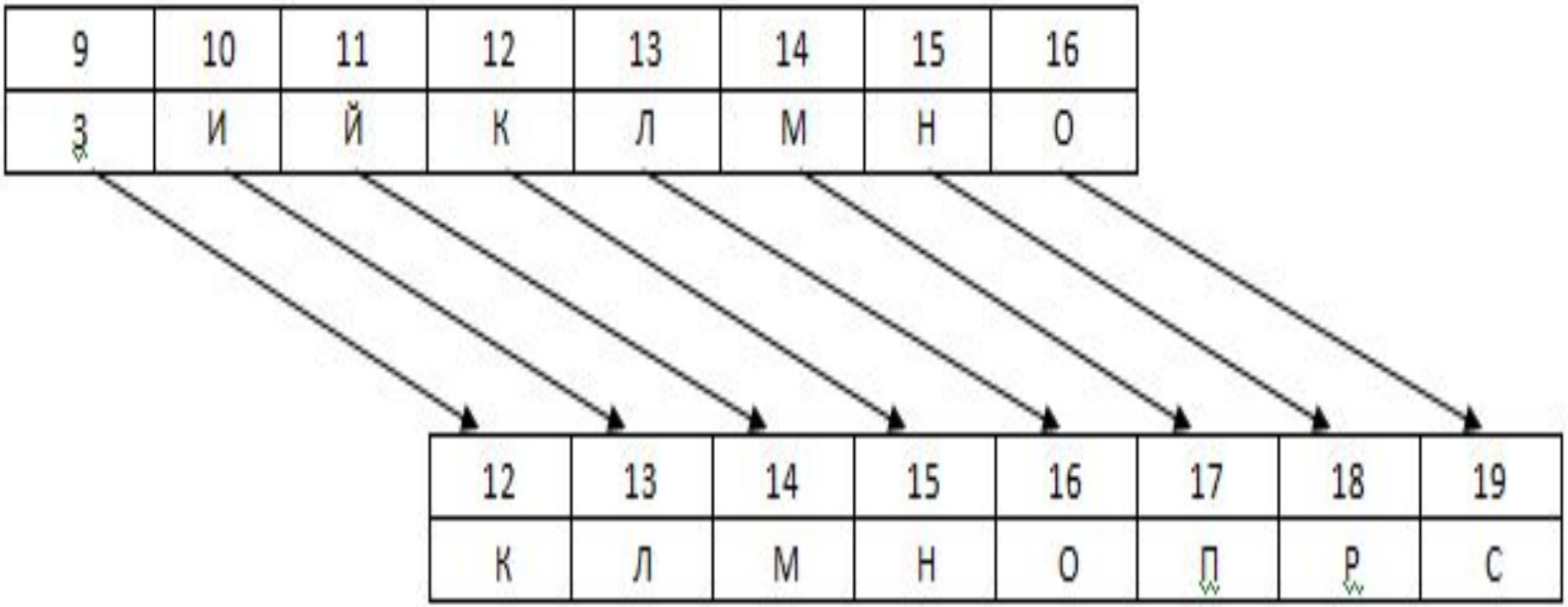
- **Криптогра́фия** (от др.-греч. κρυπτός — скрытый и γράφω — пишу) — наука о методах обеспеченияконфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.
- Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую

Как все начиналось…

- В основном древние методы криптографии использовались для защиты от злоумышленников, либо конкурентов Например, один из сохранившихся зашифрованных текстов Месопотамии представляет собой табличку, написанную клинописью и содержащую рецепт изготовления глазури для гончарных изделий. В этом тексте использовались редко употребляемые значки, игнорировались некоторые буквы, употреблялись цифры вместо имен. В рукописях древнего Египта часто шифровались медицинские рецепты. Да и найденный не так давно рецепт изготовления пива тоже был зашифрован древними египтянами.
- Первоначально методы шифрования были довольно примитивными. Например, в древнеиндийских рукописях упоминались системы замены гласных букв согласными и наоборот. Юлий Цезарь в совей секретной переписке с отдаленными провинциями Рима пользовался так называемым «кодом Цезаря»-циклической перестановкой букв в сообщении

Месопотамия

Код Цезаря



Древняя Греция

В постепенном движении к применению компьютерных средств криптографии человечество пришло через этапы использования различных механических устройств. В Спарте в 5-4 веках до н.э. использовалось одно из первых шифровальных приспособлений- Сциталла. Это был жезл цилиндрической формы, на который наматывалась бумажная лента. Вдоль ленты писался текст. Прочесть его можно было с использованием аналогичного цилиндра, который имелся у получателя сообщения. Вскрыть такой шифр было несложно

И снова Древняя Греция

- По легенде, Аристотель предложил первый способ чтения зашифрованных посланий с использованием конуса. Таким образом, он являлся своеобразным прародителем будущего поколения специалистов по взлому систем защиты, в том числе и компьютерных и криптографических. Еще одним способом шифрования являлась табличка Энея. Шифрование велось с помощью нарисованного на табличке алфавита и нити, наматываемой на специальные выемки. Узелки показывали на буквы в словах послания. Расшифровать такие сообщения без использования аналогичных табличек никаким злоумышленникам не удавалось.

Криптография на Востоке

- Значительное развитие криптография получила в период расцвета арабских государств (8 век н.э.) Слово «шифр» арабского происхождения, так же как и слово «цифра». В 855 году появляется «Книга о большом стремлении человека разгадать загадки древней письменности», в которой приводятся описания систем шифров, в том числе и с применением нескольких шифроалфавитов. В 1412 году издается 14-томная энциклопедия, содержащая обзор всех научных сведений-«Шауба аль-Аша». В данной энциклопедии содержится раздел о криптографии, в котором приводятся описания всех известных способов шифрования. В этом разделе имеется упоминание о криптоанализе системы шифра, который основан на частотных характеристиках открытого и шифрованного текста. Приводится частота встречаемости букв арабского языка на основе изучения текста Корана- то, чем в настоящее время и занимаются криптологи при расшифровке текстов.

Эпоха «Черных кабинетов»

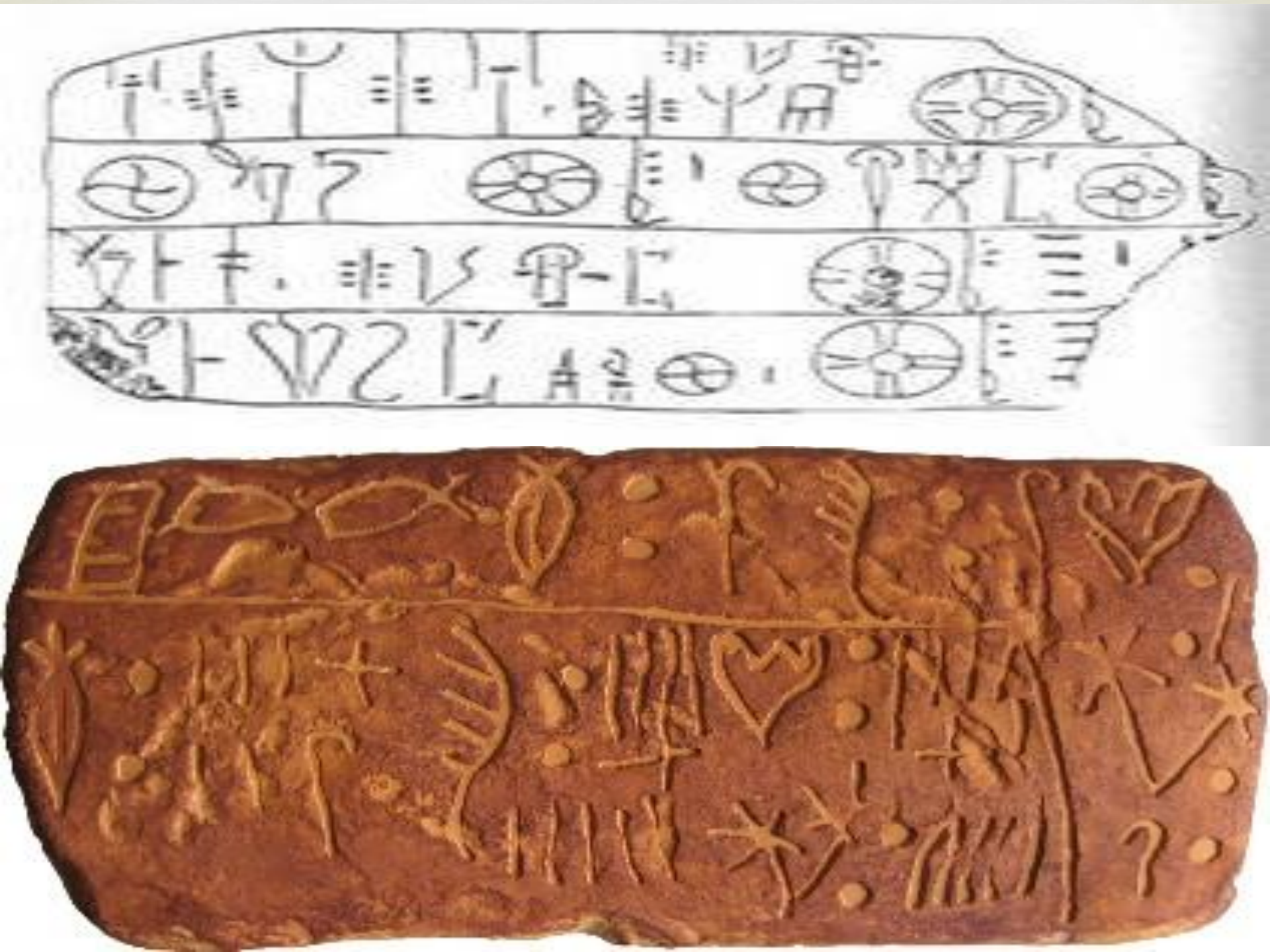
- В истории криптографии 17-18 в. называют эрой «черных кабинетов». Именно в этот период во многих государствах Европы получили развитие дешифровальные подразделения, названные «Черными кабинетами». Криптографы стали цениться чрезвычайно. Тем не менее, в канцелярии Папы Римского работники шифровального отделения после года службы подлежали физическому уничтожению. Изобретение в середине 19-го века телеграфа и других технических средств связи дало новый толчок к развитию криптографии. Информация передавалась в виде токовых и бестоковых посылок, т.е. в двоичном виде! Возникла проблема рационального представления информации, потребность в высокоскоростных способах шифрования и корректирующих кодах, необходимых в связи с неизбежными ошибками при передаче сообщений, что является необходимыми условиями и при работе с информацией в компьютерных сетях.

Вторая мировая война

- Две мировые войны 20-го века значительно способствовали развитию систем криптографии. Причина этого состояла в необычайном росте объема шифропереписки, передаваемой по различным каналам связи. Криптоанализ стал важнейшим элементом разведки. Но развитие этой отрасли науки временно прекратилось Это было связано с тем, что ручное шифрование полностью исчерпала себя и с тем, что техническая сторона криптоанализа требовала сложных вычислений, обеспечиваемых только компьютерной техникой, которая в те времена еще не существовала.

70-е годы

- В семидесятых годах 20-го века произошли события, значительно повлиявшие на дальнейшее развитие криптографии в мире- это принятие и опубликование первого стандарта шифрования данных (DES) и родилась криптография «с открытым ключем». Эти события были вызваны потребностями бурно развивающихся средств компьютерной техники и коммуникации, для защиты которых требовались легко доступные и надежные средства защиты. Но с появлением средств защиты возник новый класс преступлений, направленный на взлом защиты систем передачи данных и получение доступа к нужной преступнику информации и на сокрытие




image(c)http://www.flickr.com/photos/jvdc/