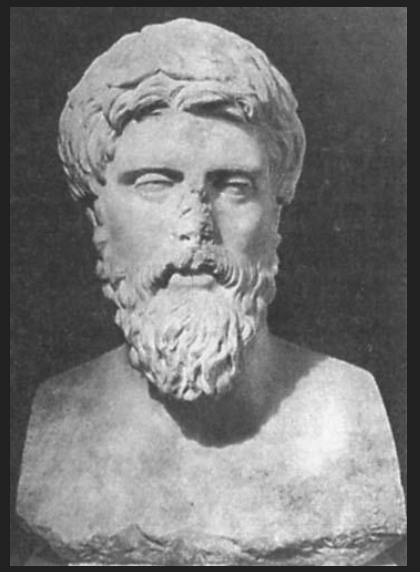
История криптографической деятельности

Определение криптографии

- Криптография – наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, а также невозможности отказа от авторства

Скиталь

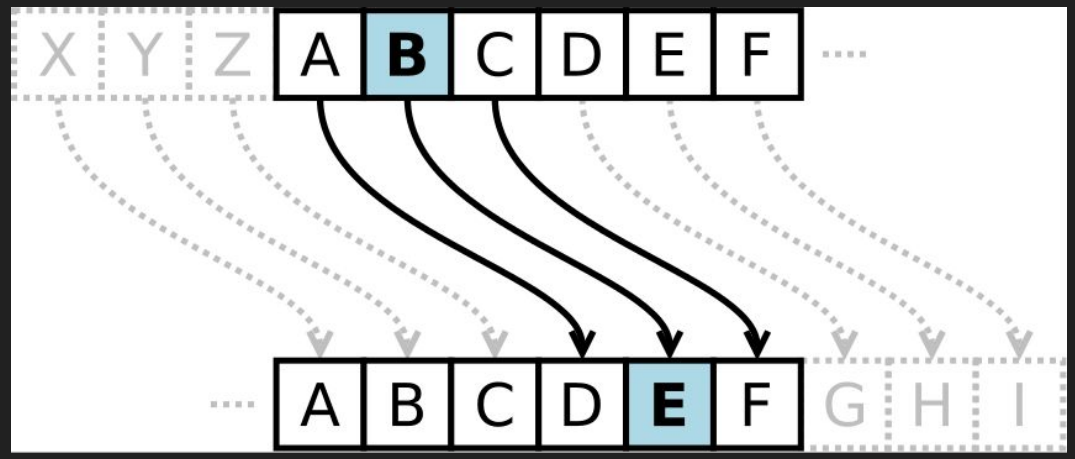
- Во времена Плутарха (45 – 127 г. н.э) использовалось шифрующее устройство - Скиталь

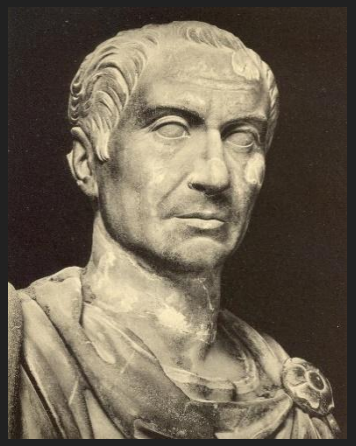


Скиталь - инструмент, используемый для осуществления перестановочного шифрования, в криптографии известный также как *шифр Древней Спарты*. Представляет собой цилиндр и узкую полоску пергамента, на которой писалось сообщение, обматывавшуюся вокруг него по спирали

Шифр Цезаря

- Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.





Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Квадрат Полибия

- Оригинальный код простой замены, одна из древнейших систем кодирования, предложенная Полибием (греческий историк и государственный деятель) . Данный вид кодирования изначально применялся для греческого алфавита[1], но затем был распространен на другие языки.
- При шифровании в таблице ищется очередная буква открытого текста, а в шифротекст записывается та буква, которая расположена ниже нее в том же столбце. Если буква текста оказывается в нижней строке таблицы, то для шифротекста берут самую верхнюю букву того же столбца.
- Для расшифровки обязательно необходимо знать, как был заполнен квадрат Полибия изначально. Если эта информация известна, то в нем ищется буква шифротекста и выписывается стоящая сверху нее в том же столбце. Если буква оказывается в верхней строке таблицы, то берется самая нижняя буква того же столбца

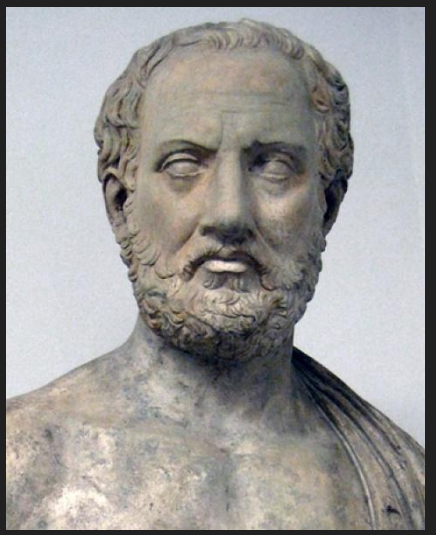
Квадрат Полибия

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ж	З	И	Й	К	Л
3	М	Н	О	П	Р	С
4	Т	У	Ф	Х	Ц	Ч
5	Ш	Щ	Ь	Ы	Ъ	Э
6	Ю	Я				

Пример:

Г Р Е Ц И Я

14 35 16 45 23 62



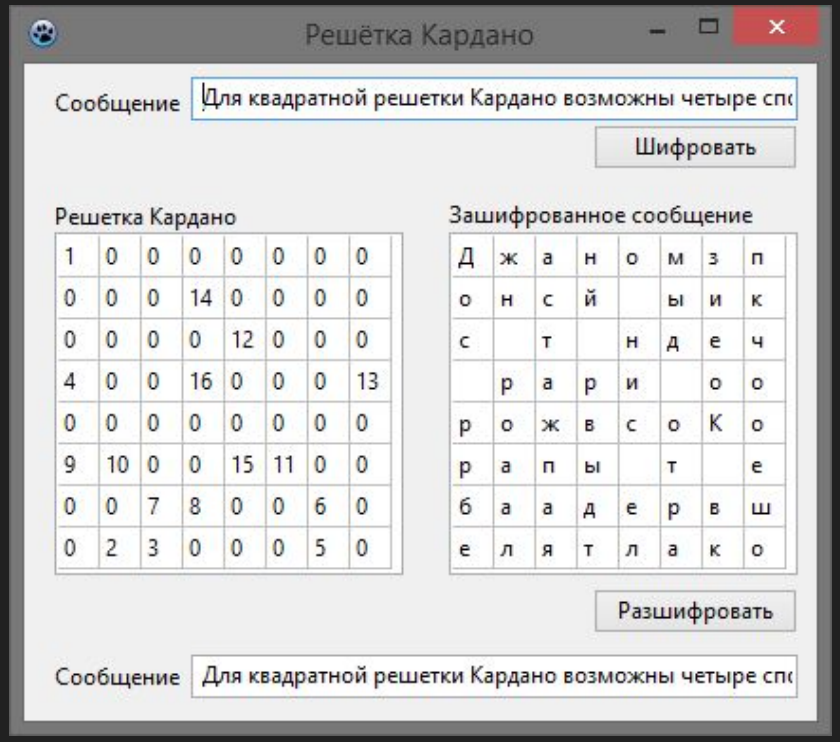
Роджер Бэкон

- Французский монах и философ, живший в XII в. описал семь систем секретного письма. Большинство шифров в те времена применялись для закрытия научных записей.

Шифр Аве Мария

- В XV веке аббат Тритемий (Германия) сделал два новаторских предложения в области криптографии: он предложил шифр «Аве Мария» и шифр, построенный на основе периодически сдвигаемого ключа.
- Шифр «Аве Мария» основан на принципе замены букв шифруемого текста на заранее оговоренные слова. Из этих сообщений составлялось внешне «невинное» сообщение. Приведем пример.
- **Заменим буквы Е, Н, Т на следующие слова: Е = «ЗЕЛЕНЫЙ», «ЖДУ», «МОЙ»; Н = «И», «Я», «ЗДЕСЬ»; Т = «ДОМА», «ВЕЧЕРОМ», «ОКОЛО», «КЛЮЧ»**
- Тогда отрицательный секретный ответ «нет» на заданный вопрос может иметь несколько «невинных» вариантов: «Я жду дома», «Я жду вечером», «Здесь мой ключ».

Решётка Кардано



Решетка Кардано							
1	0	0	0	0	0	0	0
0	0	0	14	0	0	0	0
0	0	0	0	12	0	0	0
4	0	0	16	0	0	0	13
0	0	0	0	0	0	0	0
9	10	0	0	15	11	0	0
0	0	7	8	0	0	6	0
0	2	3	0	0	0	5	0

Зашифрованное сообщение							
Д	ж	а	н	о	м	з	п
о	н	с	й		ы	и	к
с		т		н	д	е	ч
	р	а	р	и		о	о
р	о	ж	в	с	о	К	о
р	а	п	ы		т		е
б	а	а	д	е	р	в	ш
е	л	я	т	л	а	к	о

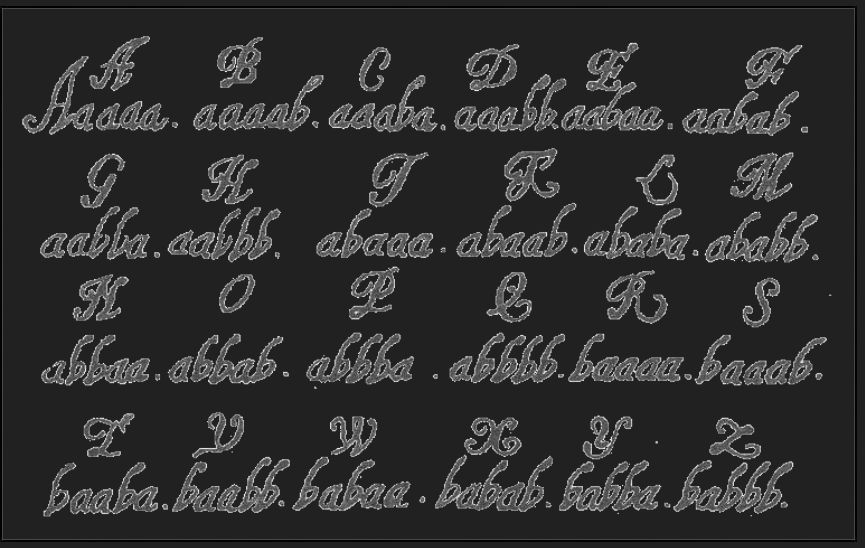
Инструмент шифрования и дешифрования, представляющий собой специальную прямоугольную (в частном случае — квадратную) таблицу-карточку, часть ячеек которой вырезана.

Сделана из листа картона или пергамента, или же из тонкого металла. Чтобы обозначить линии письма, бумагу разлиновывают, и между этими линиями вырезают прямоугольные области через интервалы произвольной длины.

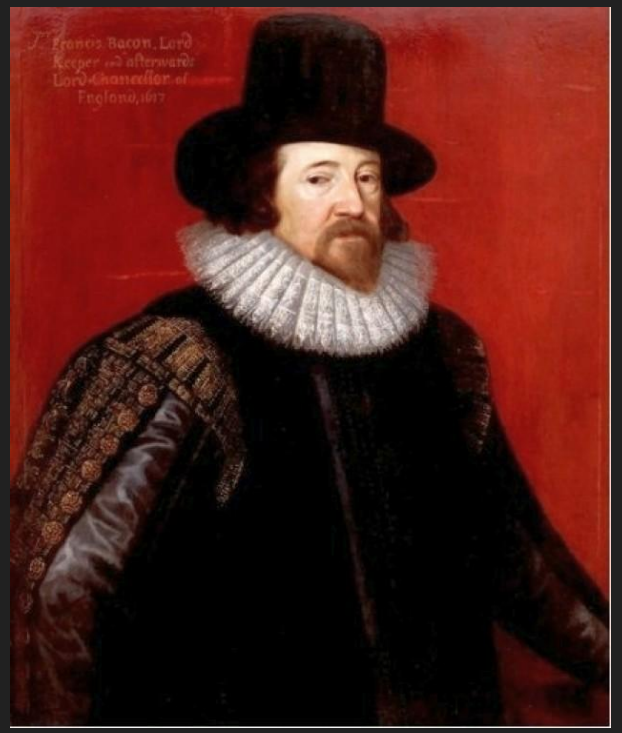
Шифрующий помещает решётку на лист бумаги и пишет сообщение в прямоугольных отверстиях, в которых помещается отдельный символ, слог или целое слово. Исходное сообщение оказывается разделённым на большое число маленьких фрагментов. Затем решётка убирается и пустые места на бумаге заполняются посторонним текстом так, чтобы скрываемый текст стал частью криптотекста.

Итальянский математик Джеромало Кардано

Шифр Бэкона



- Метод сокрытия секретного сообщения, придуманный Фрэнсисом Бэконом в начале XVII века.
- Шифр базируется на двоичном кодировании алфавита символами «A» и «B», которым можно сопоставить «0» и «1». Затем секретное послание «прячется» в открытом тексте, с помощью одного из способов сокрытия сообщений

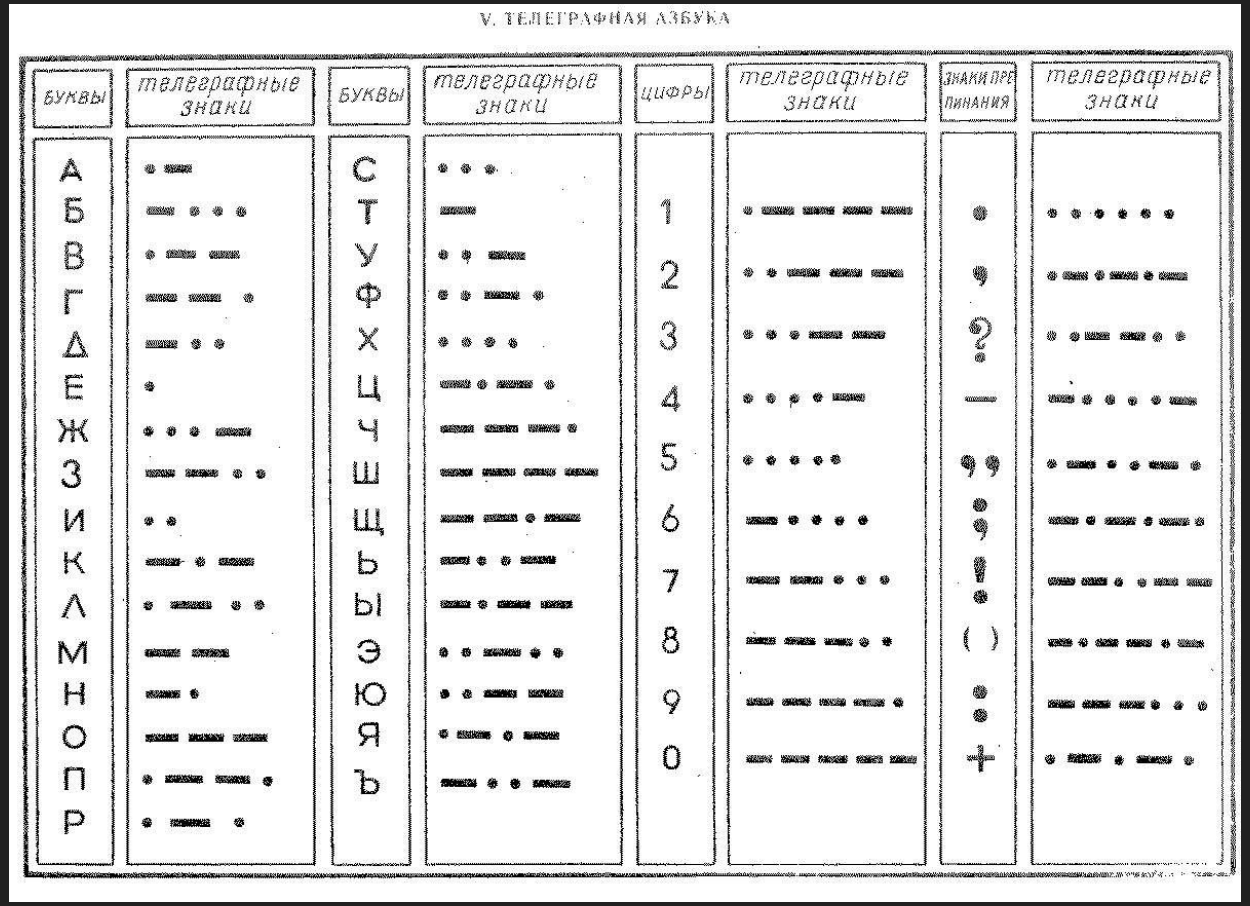


Шифрование Гаусса

- Великий математик Карл Гаусс (1777-1855) создал шифр, в котором использовалась рандомизация случайного текста.
- Такой текст можно преобразовать в другой текст, содержащий символы большего алфавита, путем замены часто встречающихся букв случайными символами из соответствующих определенных им групп. В получающемся тексте все символы большего алфавита встречаются с примерно одинаковой частотой.

Азбука Морзе

- Перечень сигналов, состоящий из ряда цифр, букв алфавита, знаков препинания и прочих символов, являющихся способом знакового кодирования. Сам код состоит из точек и тире, воспроизводящихся с помощью радиосигналов или прерыванием постоянного электрического тока. Свое название Азбука Морзе получила в честь Сэмюэла Морзе.



Современные методы криптографии

- Для современной криптографии характерно использование открытых алгоритмов шифрования, предполагающих использование вычислительных средств. Известно более десятка проверенных алгоритмов шифрования, которые при использовании ключа достаточной длины и корректной реализации алгоритма криптографически стойки. Распространенные алгоритмы:

- симметричные DES, AES, ГОСТ 28147-89, Camellia, Twofish, Blowfish, IDEA, RC4 и др.;
- асимметричные RSA и Elgamal (Эль-Гамаль);
- хэш-функций MD4, MD5, MD6, SHA-1, SHA-2, ГОСТ Р 34.11-94.
- Криптографические методы стали широко использоваться частными лицами в электронных коммерческих операциях, телекоммуникациях и многих других средах.

- Во многих странах приняты национальные стандарты шифрования. В 2001 году в США принят стандарт симметричного шифрования AES на основе алгоритма Rijndael с длиной ключа 128, 192 и 256 бит. Алгоритм AES пришёл на смену прежнему алгоритму DES, который теперь рекомендовано использовать только в режиме Triple DES. В Российской Федерации действует стандарт ГОСТ 28147-89, описывающий алгоритм блочного шифрования с длиной ключа 256 бит, а также алгоритм цифровой подписи ГОСТ Р 34.10-2001.