Средневековая криптография

Выполнила: Ле Йен Ни

МНб-1601-01-00

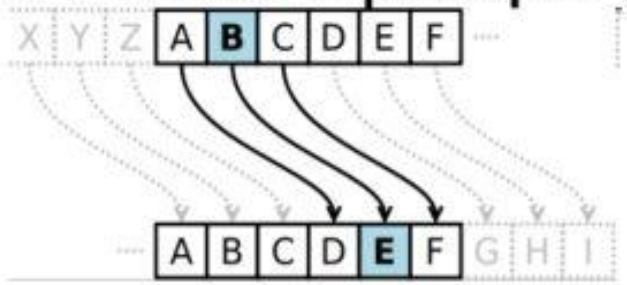
Криптогра́фия (от др.-греч. κρυπτός — скрытый и γράφω — пишу) — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.

Способы защиты информации

- Охрана документа (носителя информации) физическими лицами, его передача специальным курьером.
- «Стеганография» заключается в сокрытии самого факта наличия секретной информации.
- Третий способ защиты информации заключался в преобразовании смыслового текста в некий хаотический набор знаков (букв алфавита).

ШИФР Гая Юлия Цезаря

- Шифр Гая Юлия Цезаря (замена)



- Шифр перестановки

1	2	3	4	5
3	2	5	1	4

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
С	В	Я	Щ	Е	Н	Н	А	Я	Р	И	М	С	К	А	Я	И	М	П	Е	Р	И	Я	Б	В

Щ	В	С	Е	Я	Я	Н	Н	Р	А	К	М	И	А	С	П	И	Я	Е	М	Б	И	Р	В	Я

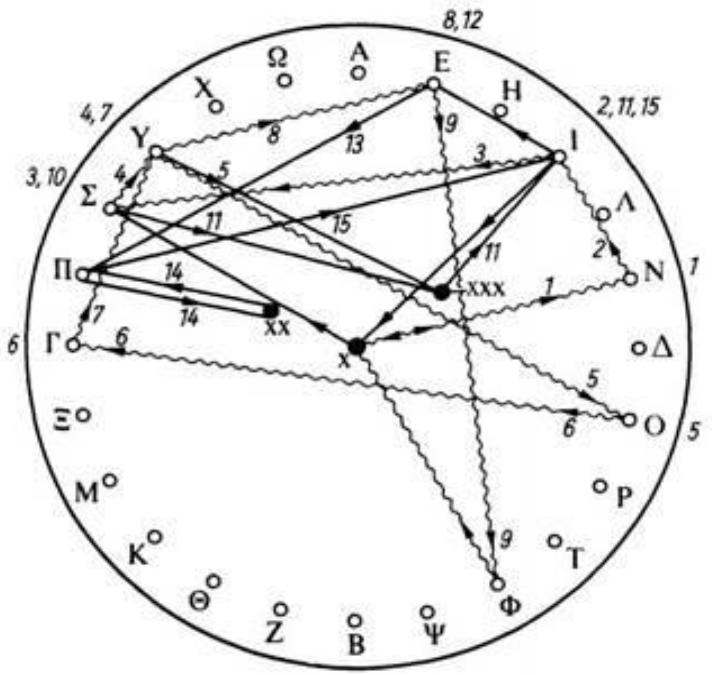
ПРИБОР Сцитала

Прибор, реализующий шифр перестановки – Сцитала.

Ключ шифра – диаметр цилиндра и его длина.

ДИСК Энея

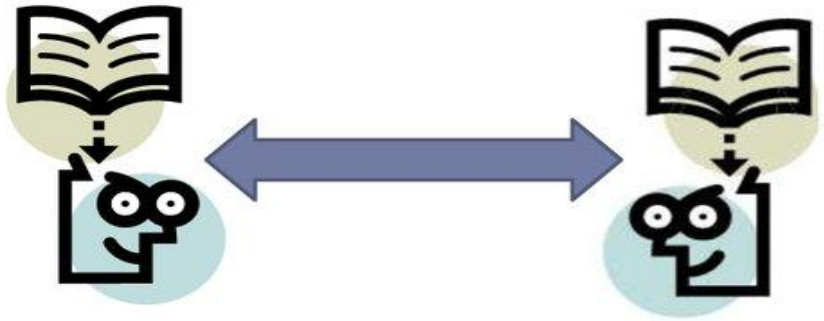
- Диск Энея представлял собой диск диаметром 10-15 см с отверстиями по числу букв алфавита. Для записи сообщения нитка протягивалась через отверстия в диске, соответствующим буквам сообщения. При чтении получатель вытягивал нитку, и получал буквы, правда, в обратном порядке. Эней также предусмотрел способ быстрого уничтожения сообщения – для этого достаточно выдернуть нить, закреплённую на катушке в центре диска.



КНИЖНЫЙ шифр

Ключ шифра – книга

Плюс: его невозможно разгадать, не имея под рукой книги шифровальщика.
Минус: необходимость всегда использовать именно эту книгу.



КВАДРАТ Полибия

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Зашифруем слово APPLE:
11.35.35.31.15

Квадрат Полибия – способ кодирования букв алфавита с целью его приведения к виду, удобному для передачи по каналу связи. Данный вид кодирования изначально применялся для греческого алфавита, но затем был распространён на другие языки. Порядок расположения символов в Квадрате Полибия и является секретным ключом.