МБОУ «Кадетская школа «Патриот»

IT - криптограф

Учитель информатики и ИКТ
Калиновский В.Г.

Криптология
(*kryptos - тайный, logos - наука*)

Криптография

Разработка методов преобразования (шифрования) информации с целью ее защиты от незаконных пользователей

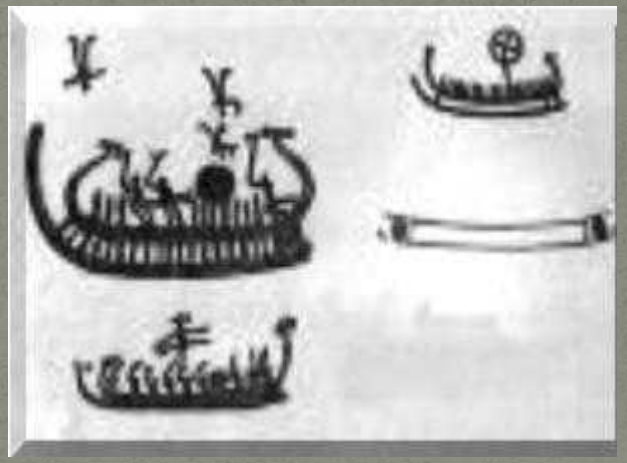
Криптоанализ

Исследование возможности расшифровывания информации без знания ключей

Калиновский В.Г.

Простейшие методы шифрования

Общество, в котором живёт человек, на протяжении своего развития имеет дело с информацией. Она накапливается, перерабатывается, хранится, передаётся.



Защита информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен.

Приватная, конфиденциальная, секретная информация

- государственная тайна;
- военная тайна;
- коммерческая тайна;
- юридическая тайна;
- врачебная тайна.

Шифровальные устройства

Скитала – греческое шифровальное устройство

(V-VI вв. до н.э.)

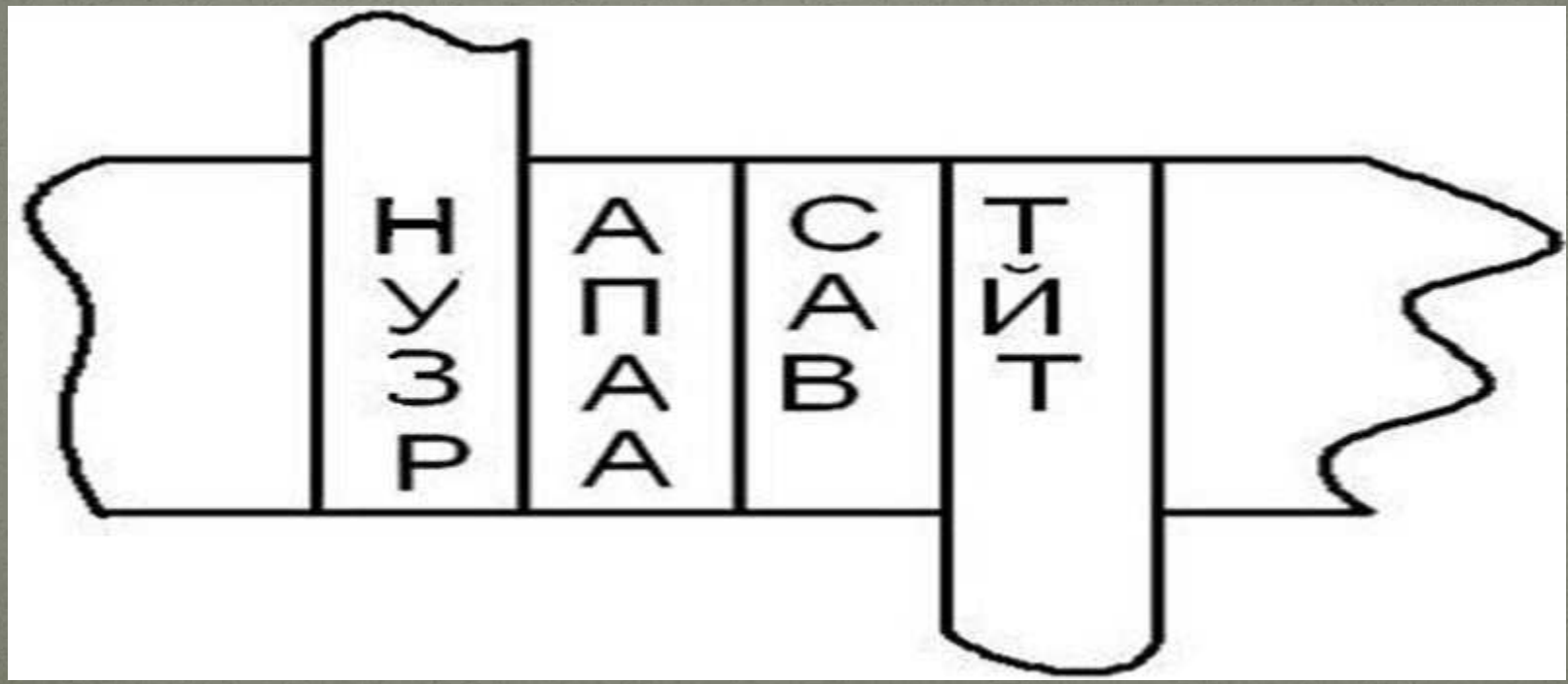
Скитала

Алгоритм шифрования: на жезл наматывают ленту и пишут открытый текст вдоль палочки по намотанной ленте. На смотанной ленте получается шифротекст — удобно и быстро. Толщина жезла и алфавит являются ключом шифра.

Проверь себя

Расшифруйте сообщение, переданное спартанцу в V век до н. э.

НУЗРАПАДАСАВТЙТ



Шифр Цезаря

Сообщение об одержанной им победе
выглядело так:

YHQL YLGL YLFL

«Veni, vidi, vici» -

«Пришел, увидел, победил» (лат.)
Г.Ю.Цезарь

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

Император Август

(I в. до н. э.) в своей переписке заменял первую букву на вторую, вторую - на третью и т.д., наконец, последнюю - на первую:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

BCDEFGHIJKLMNOPQRSTUVWXYZA

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

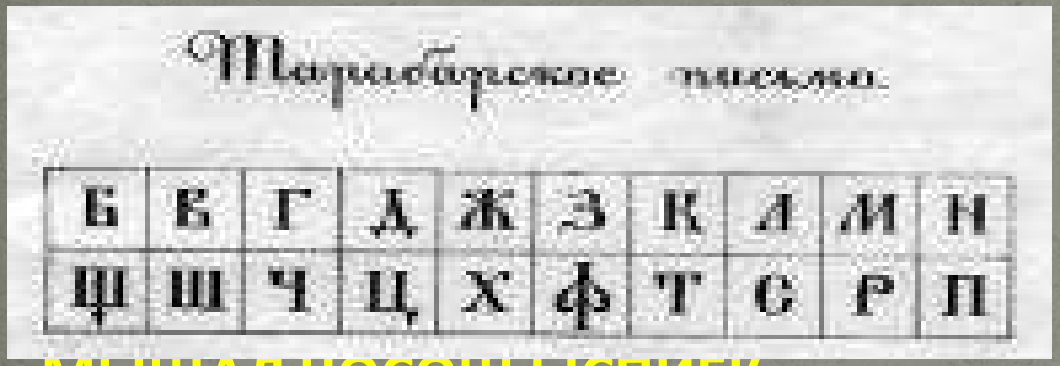
«Festina lente»

«Торопись медленно» (лат.)

Тайнопись в России

Первое известное применение тайнописи в России относится к XIII в.

Эту систему называли
«тарабарской грамотой».
В этой системе согласные буквы заменяются по схеме:


Тарабарское письмо.

б	в	г	д	ж	з	к	л	м	н
щ	ш	ч	ц	х	ф	т	с	р	п

«МЫЩАЛ ЧОСОШ ЫСПИЕК»

«Рыба с головы гниет»

Цифирь

В эпоху Петра I в качестве системы шифрования широко употреблялась «цифирь» или «цифирная азбука- это шифр простой замены

а	б	в	г	д	е	ж
з	и	к	л	м	н	о
п	р	с	т	у	ф	х
ѡ	ц	ч	ш	щ	ъ	ы
ь	ѣ	ю	я			

Отечественные криптоаналитики вскрыли шифрованный приказ Гитлера о наступлении под Курском

Роторная шифровальная машина Энигма

Разные модификации Энигмы использовались германскими войсками с конца 1920-х годов до конца Второй мировой войны. Эта машина осуществляла сложное электромеханическое полиалфавитное шифрование.

Криптография точная наука

В конце XIX века криптография начинает приобретать черты точной науки, а не только искусства, ее начинают изучать в военных академиях. В одной из них был разработан свой собственный военно-полевой шифр, получивший название "Линейка Сен-Сира".

В 80-х годах XIX века ОГЮСТ КЕРКГОФФС издал книгу "Военная криптография" объемом всего в 64 страницы, но они обессмертили его имя в истории криптографии. В ней сформулированы шесть конкретных требований к шифрам. Все эти требования актуальны и в наши дни.

Электронные шифраторы

Во второй половине XX века, вслед за развитием элементной базы вычислительной техники, появились электронные шифраторы. Сегодня они составляют подавляющую долю средств шифрования, удовлетворяя все возрастающим требованиям по надежности и скорости шифрования. В семидесятых годах был принят и опубликован первый стандарт шифрования данных (DES), "легализовавший" принцип Керкгоффса в криптографии; после работы американских математиков У. ДИФФИ и М. ХЕЛЛМАНА родилась "новая криптография"— криптография с открытым ключом.

Подготовка криптографов

В перечень специальностей высшего образования включено 6 специальностей блока 070000 (информационная безопасность).

В МГУ им. М.В. Ломоносова производится обучение по специальностям «Математические методы защиты информации» и «Программное обеспечение защиты информации».

В СГУ им. Н.Г. Чернышевского имеется кафедра подготовки по специальности 090301 "Компьютерная безопасность»

Выводы

Криптография сегодня – это наука об обеспечении безопасности данных или, как говорят, информационной безопасности.

Шифрование, основное действие в криптографии, позволяет обеспечить конфиденциальность, сохраняя информацию втайне от того, кому она не предназначена.