

Информационные процессы



Основные информационные процессы

Хранение информации



Передача информации



Обработка информации



Хранение информации:

Люди хранят информацию в собственной памяти, которую можно назвать «оперативной», т.е. «быстрой».

Человек быстро воспроизводит сохраненные в памяти знания.

Поэтому память человека можно еще назвать внутренней памятью



Хранение информации:

Информацию, сохраненную на внешних носителях, таких как: записная книжка, справочники, энциклопедии, диски и т.д. можно назвать внешней памятью человека.



Передача информации:



Источник передает информацию (отправляет).
Приемник – получает (воспринимает).

Передача информации:



Передача информации от источника к приемнику всегда происходит через канал передачи.

В процессе передачи информация может искажаться или теряться, если информационные каналы имеют плохое качество или на линии связи действуют помехи (шумы).

Обработка информации:

Процесс обработки информации связан с получением новой информации, изменением формы или структуры имеющейся информации.

Кодирование

Преобразование представления информации из одной символьной формы в другую, удобную для ее хранения, передачи и обработки, без изменения содержания информации – это кодирование.

Обработка информации:

Кодирование

Шифрование

**Сортировка
(упорядочивание)**

Структурирование

***Важным информационным процессом является
поиск информации.***



***Информационные процессы протекают и в
живой природе:***



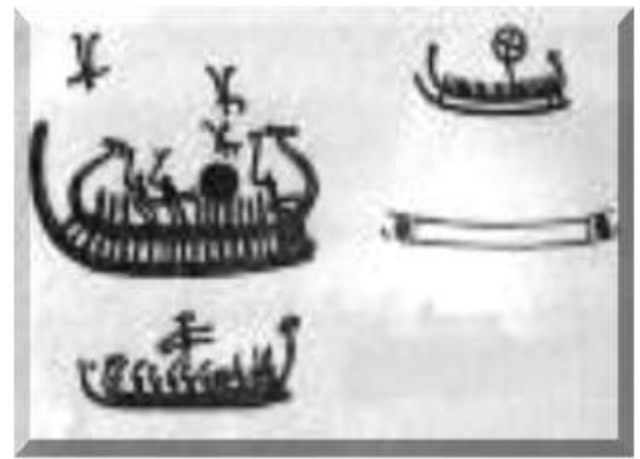
Криптография



Криптография (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.



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



Хитроумный способ шифрования был изобретён в древней Спарте во времена Ликурга (V век до н.э.).

Для зашифровывания текста использовалась Сциталла - жезл цилиндрической формы, на который наматывалась лента из пергамента. Вдоль оси цилиндра построчно записывался текст, лента сматывалась с жезла и передавалась адресату, имеющему Сциталлу такого же диаметра.

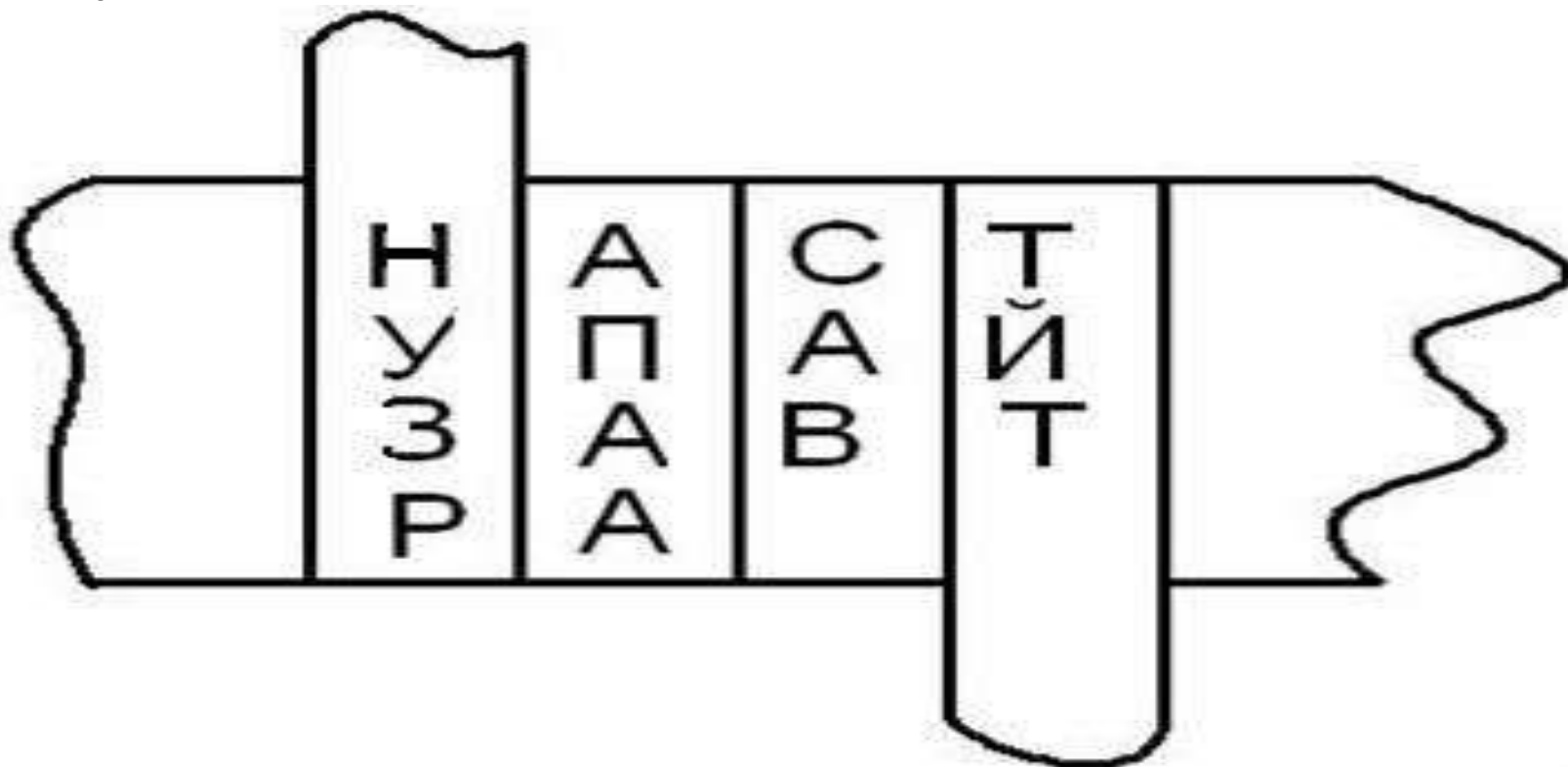
Этот способ осуществлял перестановку букв сообщения. Ключом шифра служил диаметр Сциталлы.

АРИСТОТЕЛЬ придумал метод вскрытия такого шифра. Он изобрёл дешифровальное устройство «Антисциталла».



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

НУЗРАПААСАВТЙТ



Греческий писатель ПОЛИБИЙ использовал систему сигнализации, которая применялась как метод шифрования. С его помощью можно было передавать абсолютно любую информацию. Он записывал буквы алфавита в квадратную таблицу и заменял их координатами.



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

Устойчивость этого шифра была велика. Основная причина - возможность постоянно менять в квадрате последовательность букв.

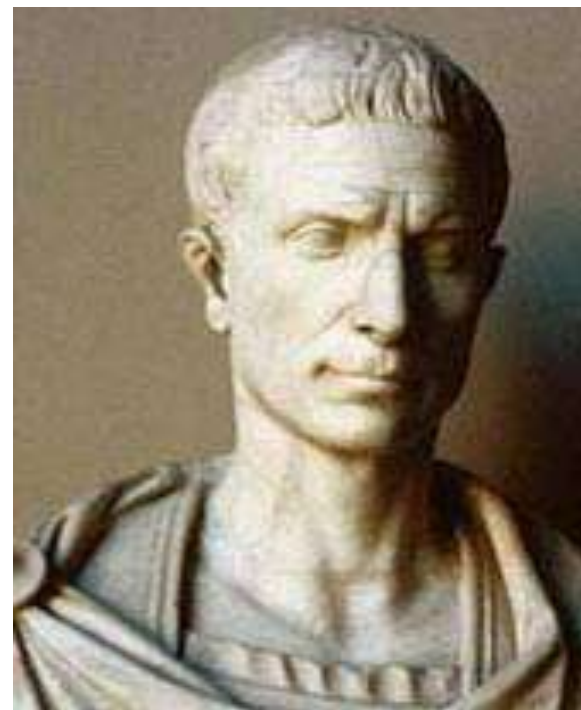
Расшифруйте сообщение,

**636443321662643611123442114254644164522
44436343265641164425566**

**Я умею
работать
с шифром!
А ты?**

**Алгоритм шифрования:
первая цифра кода –
номер строки,
вторая – номер столбца.**

**Особую роль в сохранении тайны
сыграл способ шифрования,
предложенный ЮЛИЕМ ЦЕЗАРЕМ
и описанный им в «Записках о
галльской войне» (1 век до н.э.)
Ключом в шифре Цезаря
является величина сдвига на 3.**



Закодируем слово КОД

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

Получаем слово

Расшифруйте сообщение

ТУЛЫИО, ЦЕЛЖЗО,ТСДЗЖЛО!

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

***Алгоритм шифрования: читать
четвертую букву вместо первой.***

Пришёл, увидел, победил!

Научные методы в криптографии впервые появились в арабских странах. Арабского происхождения и само слово шифр (от арабского «цифра»). Арабы первыми стали заменять буквы цифрами с целью защиты исходного текста. Первая книга, специально посвящённая описанию некоторых шифров, появилась в 855г., она называлась «Книга о большом стремлении человека разгадать загадки древней письменности».

**Итальянский математик и философ
ДЖЕРОЛАМО КАРДАНО написал книгу "О
тонкостях", в которой имеется часть,
посвященная криптографии.**

**Кардано дает "доказательство" стойкости
шифров, основанное на подсчете числа
ключей, предлагает использовать
открытый текст в качестве ключа, и
новый шифр, "Решетка Кардано".**

**Решётка представляет собой лист из
твёрдого материала, в котором через
неправильные интервалы сделаны
прямоугольные вырезы высотой для одной
строчки и различной длины. На лист
накладывали эту решетку и записывали в
вырезы секретное сообщение. Оставшиеся
места заполнялись произвольным текстом.**



Расшифруйте сообщение, используя одну из разновидностей решётки Кардано – поворотную решётку.

Эта наука
интересная и перспективная

Увлекались тайнописью и в России. Используемые шифры - такие же, как в западных странах - значковые, замены, перестановки.

Датой появления криптографической службы в России считают 1549 год, с момента образования "посольского приказа", в котором имелось "цифирное отделение". Петр I полностью реорганизовал криптографическую службу, создав "Посольскую канцелярию".



***Расшифруйте сообщение написанное на
тарабарском языке***

Чем человек просвещеннее,
тем он полезнее своему Отечеству



Много новых идей в криптографии принес XIX век. ТОМАС ДЖЕФФЕРСОН создал шифровальную систему, занимающую особое место в истории криптографии - "дисковый шифр". Этот шифр реализовывался с помощью специального устройства - шифратора Джефферсона.



В 1817 г. ДЕСИУС УОДСВОРТ сконструировал принципиально новое шифровальное устройство, Нововведение состояло в том, что он сделал алфавиты открытого и шифрованного текстов различных длин.

Способов кодирования информации можно привести много.

Капитан французской армии ШАРЛЬ БАРБЬЕ разработал в 1819 году систему кодирования *écriture nocturne* – ночное письмо. В системе применялись выпуклые точки и тире, недостаток системы её сложность, так как кодировались не буквы, а звуки. ЛУИ БРАЙЛЬ усовершенствовал систему, разработал собственный шифр. Основы этой системы используются и сейчас.



Алфавит Брайля:

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

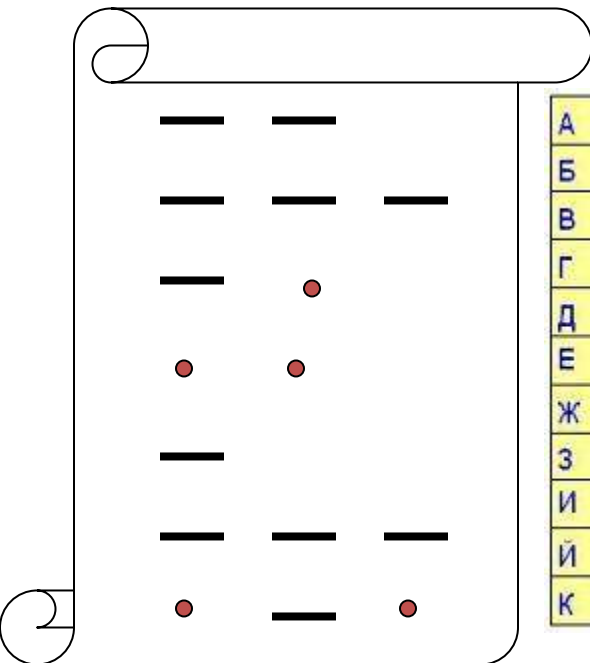
СЭМЮЕЛЬ МОРЗЕ разработал в 1838 году систему кодирования символов с помощью точки и тире.

Он является изобретателем телеграфа (1837год) – устройства в котором использовалась эта система. Самое важное в этом изобретении – двоичный код, - использование для кодирования букв только двух символов.



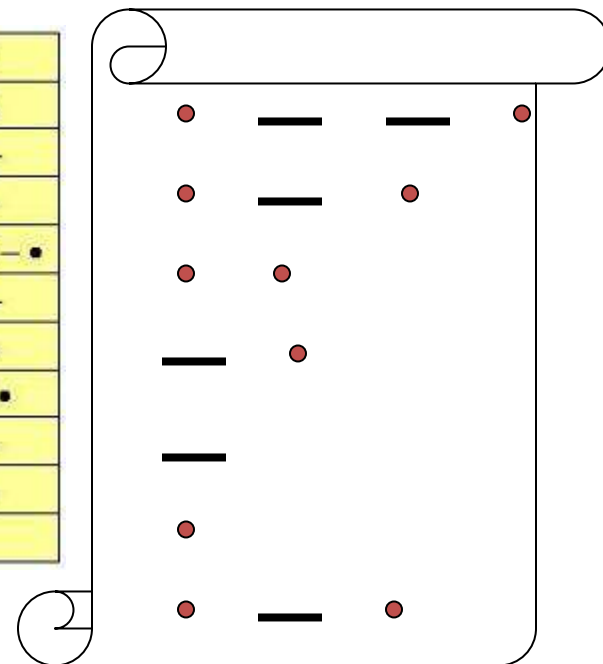
А ··	Б ···	В ---	Г ---	Д ---
Е ·	Ж ----	З ----	И ··	К ---
Л ----	М --	Н -·	О ---	П ----
Р ···	С ···	Т -	У ---	Ф ----
Х ----	Ц ----	Ч ----	Ш ---	Щ ----
Ъ ----	Ы ----	Ь ----	Э ----	
	Ю ----	Я ----		
1 ----	2 ----	3 ----	4 ----	
5 ----	6 ----	7 ----	8 ----	
9 ----	0 ----			

Расшифруйте сообщение, используя азбуку Морзе



Монитор

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



Принтер

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.

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.

Роль криптографии будет возрастать в связи с расширением ее областей приложения:

- ✓ **цифровая подпись,**
- ✓ **аутентификация и подтверждение подлинности и целостности электронных документов,**
- ✓ **безопасность электронного бизнеса,**
- ✓ **защита информации, передаваемой через Интернет и др.**

1. Акrostихи. Расшифруйте, какой поэтессе посвятил свои стихи Н. Гумилев:

Ангел лег у края небосклона,
Наклонившись, удивлялся бездне;
Новый мир был синим и беззвездным.
Ад молчал, не слышалось ни стона.
Алой крови робкое биение,
Хрупких рук испуг и содроганье
Миру снов досталось в обладанье
Ангела святое отраженье
Тесно в мире, пусть живет, мечтая
О любви, о свете и о тени,
В ужасе предвечном открывая
Азбуку своих же им откровений.

Ответ: Анна Ахматова

2. Используя «зеркальное отображение» в стихотворение С.Г. Фруга, прочитайте новое стихотворение:

**О грядущем ни намека
О минувшем – ни следа...
Отражается всегда
Лишь обманчиво глубоко
С их зеркальной глубиной
Все в очах лазурно-чистых:
И созревших страсти зной,
И мерцанье грез лучистых.
Подношу я этот дар
Ей, холодной и прекрасной,
Не пленив мечтой напрасной
Мысли свет и сердца жар.**

**3. Пользуясь ключевой таблицей,
расшифруйте следующие четверостишие и
его автора:**

3	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	.
2	П	Р	С	Т	У	Ф	Х	Ч	Ц	Ш	Щ	,
1	К	Л	М	Н	О	Ь	Ъ	Ы	Э	Ю	Я	–
	1	2	3	4	5	6	7	8	9	10	11	12

- 1) (5,3), (5,2), (2,3), (1,1), (1,3), (8,2), (1,3), (6,3), (4,2), (4,3),
(5,1), (2,1), (5,1), (3,3), (5,1), (10,1), (12,2).
- 2) (3,2), (5,1), (3,2), (4,1), (8,1), (3,3), (6,3), (4,2), (1,1), (1,3),
(3,1), (10,2), (5,2), (3,1), (11,1), (4,2), (5,3), (12,2).
- 3) (10,3), (5,1), (3,2), (8,1), (1,2), (1,3), (4,1), (3,1), (5,1), (1,1),
(2,2), (5,1), (11,3), (7,2), (3,3), (5,1), (6,3), (11,3).
- 4) (1,2), (5,1), (5,2), (4,2), (2,2), (1,3), (3,1), (5,1), (3,2), (6,3),
(4,1), (4,1), (10,3), (11,3), (3,2), (1,3), (5,3), (12,3).

Решение:

***Дуб качает головою,
Сосны ветками шумят,
И осыпан мокрой хвоей
По утрам осенний сад.***

А. Барто