

«Простейшие методы шифрования текста»



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 служил диаметр Сциталлы.

АРИСТОТЕЛЬ придумал метод вскрытия такого шифра.

Он изобрёл дешифровальное устройство «Антисциталла».



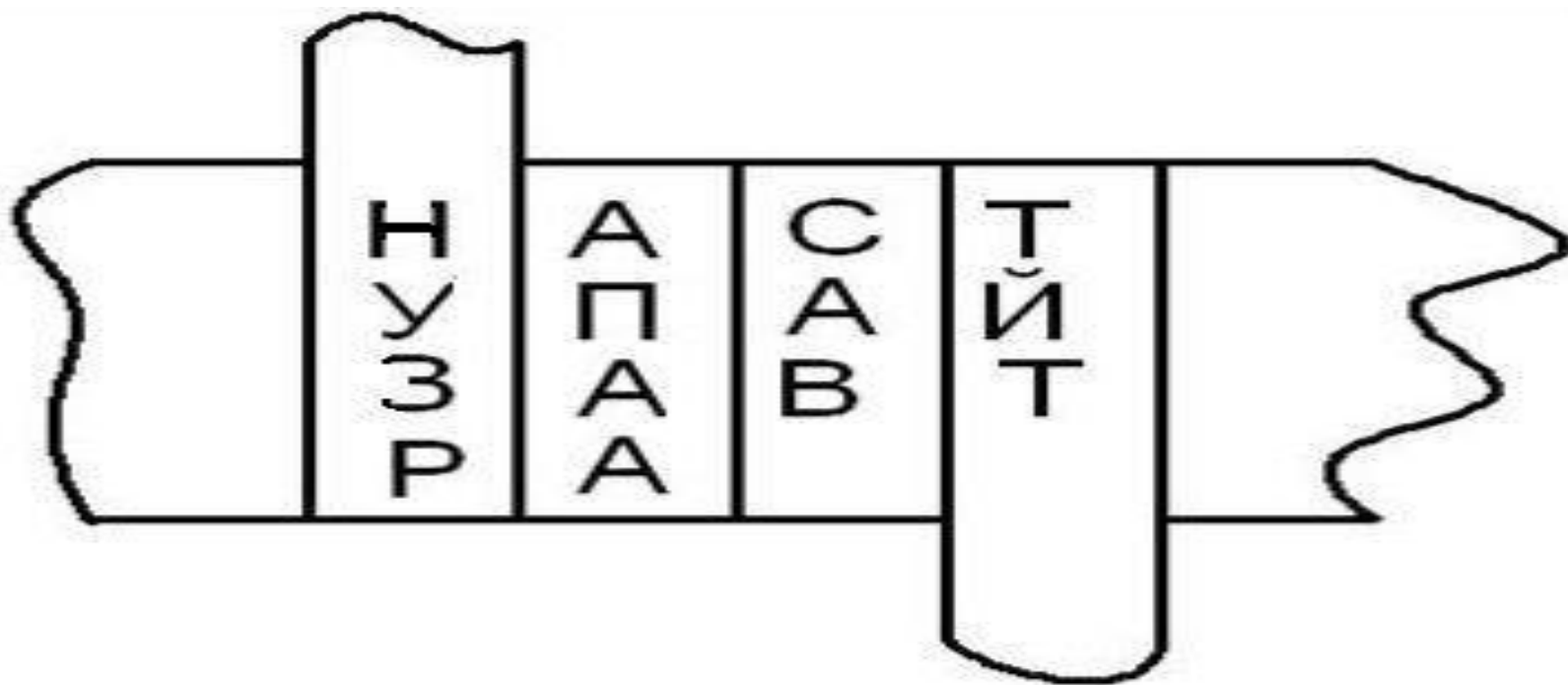
новку

шифра

Расши

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.

Проверь себя

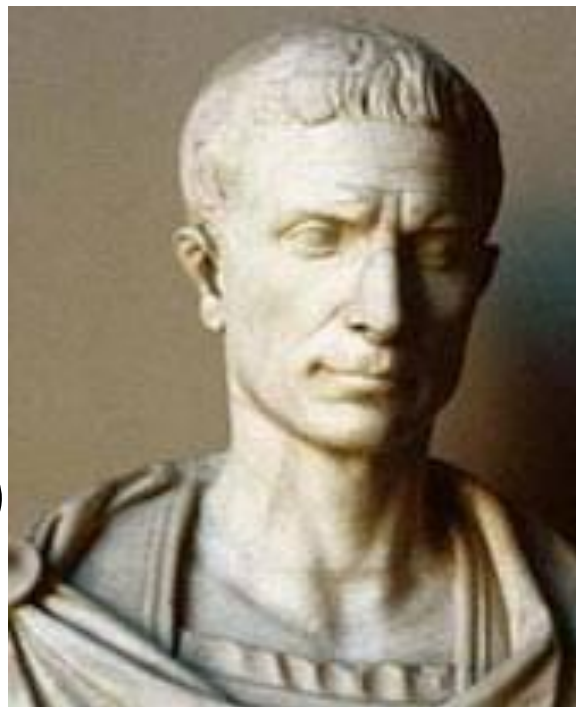
Расшифруйте сообщение,

636443321662643611123442114254644164
52244436343265641164425566

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

Проверь себя

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!

Существует несколько модификаций шифра Цезаря. Один из них алгоритм шифра Гронсфельда (созданный в 1734 году бельгийцем Хосе де Бронкхором, графом де Гронсфельд, военным и дипломатом).

Шифрование заключается в том, что величина сдвига не является постоянной, а задается ключом (гаммой).

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

При заданном ключе 317413327121 из шифротекста НСПУУСЁТЖХКА получает

Криптография

Для того, кто передаёт шифровку, важна её устойчивость к дешифрованию. Эта характеристика шифра называется криптостойкостью. Повысить криптостойкость позволяют шифры много алфавитной или многозначной замены. В таких шифрах каждому символу открытого алфавита ставятся в соответствие не один, а несколько символов шифровки.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

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 и новый шифр, "Решетка Кардано".

Решётка представляет собой лист из твердого 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.



оча

Проверь себя

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, момента образования "посольского приказа", в котором имелось "цифирное отделение". Петр I полностью реорганизовал криптографическую службу, создав "Посольскую канцелярию".



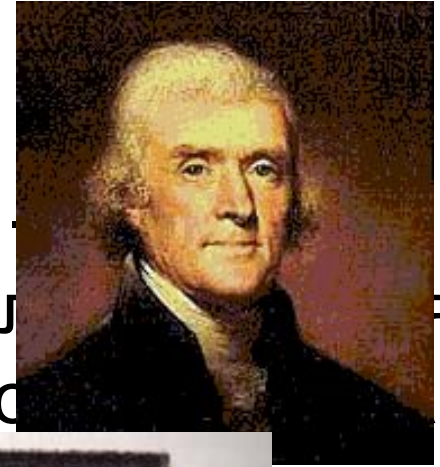
Проверь себя

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 реализован с помощью специального шифратора Десиуса.

В 1817 г. ДЕЗИУС УОДСВОРТ 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:

⠠	⠡	⠢	⠣	⠤	⠥
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	

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

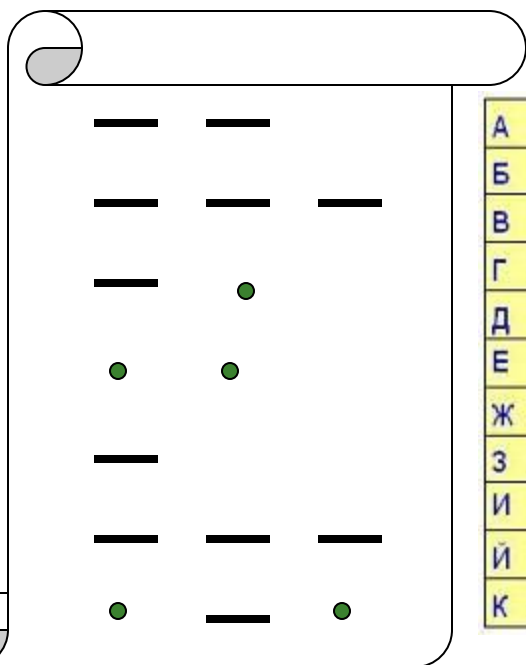
Он является изобретателем телеграфа (1837год) – устройства в котором использовалась эта система. Самое важное в этом изобретении – двоичный код, - использование для кодирования букв только двух символов.



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 ·····			

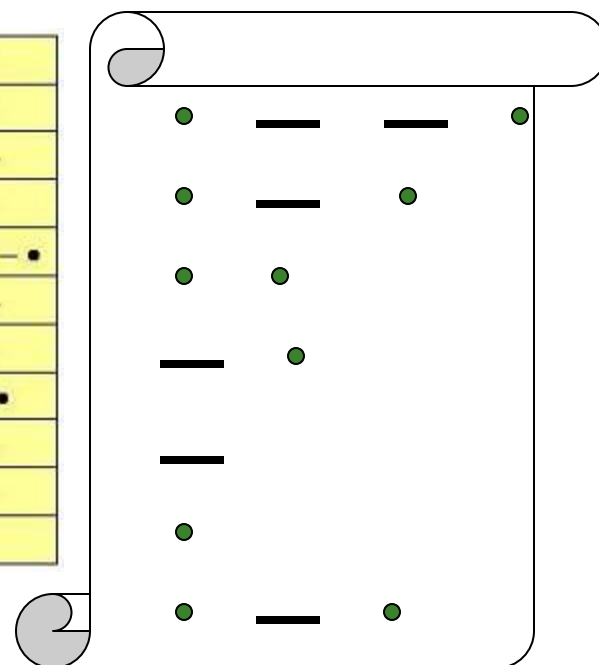
Проверь себя

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.

Проверь себя

Найдите в художественных произведениях примеры шифров. Какие «криптографические» преобразования проделывали и проделывают над своими именами и фамилиями писатели, поэты, музыканты?

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.

Знакомство с криптографией потребуется каждому пользователю электронных средств обмена информацией, поэтому криптография в будущем станет "третьей грамотностью" наравне со "второй грамотностью" - владением компьютером и информационными технологиями.
