КРИПТОГРАФИЯ

Как зашифровать послание

АВТОРЫ:
ГЛУЩЕНКО АЛЕКСАНДРА, КУЗНЕЦОВА ИРИНА,
СЛЮНКОВА ДАРЬЯ, ФРОЛОВА АНАСТАСИЯ

01 ЦЕЛЬ:

Узнать и научится, как можно зашифровать послание и какое послание будет сложнее расшифровать.

02 ПРОБЛЕМА:

Как зашифровать и дешифровать послание?

03 КЛЮЧЕВЫЕ ПОНЯТИЯ:

Криптография, шифрование, дешифрование, ключ шифра

Криптография

Слово греческое, в переводе означает тайное, скрытое (крипт) письмо (графия), или тайнопись.

Благодаря криптографии люди зашифровывают свои письма, чтобы посторонние не могли узнать о содержании письма, информация будет понятна только получателю письма. Если посторонний человек захочет узнать содержание письма, он ничего не поймет.

Подумайте и запишите, какое имело значение криптография и шифрование в мировой истории?

ИНТЕРЕСНЫЙ ФАКТ

Слово «криптография» произошло от названия подземных помещений, которые использовались для тайных встреч собраний заговорщиков и работы над шифрами. Греки называли их «спрятанные».

ШИФР ЦЕЗАРЯ

Шифр Цезаря является одним из самых распространённых шифров. Он называется так, потому что его использовал сам Юлий Цезарь ещё в I веке до нашей эры в древнем Риме для секретной переписки со своими генералами. На самом деле шифр Цезаря — это не один шифр, а целых тридцать два, использующих один и тот же принцип!

КАК ЗАШИФРОВАТЬ ПОСЛАНИЕ?

Самый простой его вариант - это когда вместо каждой буквы ставится следующая по алфавиту: вместо «а» - «б», вместо «ё» - «ж», а вместо «я» - «а».Алфавит сдвигается на одну букву. Таких смещений может быть 32. В таком случае или называют число смещения (в данном случае 1), или то, какая буква на какую заменяется (а-б). Можно шифровать на 2 или а-в. Сам Цезарь использовал перестановку на 3 или а-г, если бы говорил на русском языке.

ЗАШИФРУЙТЕ ТЕКСТ, ИСПОЛЬЗУЯ ШИФР ЦЕЗАРЯ

«На развитие способов защиты письменной информации большое влияние оказывает состояние средств связи. В то время была почта. До конца пятнадцатого века послания отправлялись со специальным курьером — гонцом. С начала шестнадцатого века стала распространяться так называемая ямская гоньба (специальная почтовая служба в России), однако тайные письма пересылались все равно со специальными гонцами. Для защиты посланий использовались особые печати. Такие печати с надписью «ДЬНЕСЛОВО», что переводится как «скрытое, тайное слово», были у киевских князей Святополка Изяславича, Мстислава Владимировича, Александра Невского и других.»

Татьяна Соболева
«История шифровального дела в России»

ТАРАБАРСКАЯ ГРАМОТА

Шифр, широко использовавшийся в древнерусских летописях

Представляет собой простейший шифр замены без ключа. Согласные в алфавите делят на две равные части, и первую пишут строкой в алфавитном порядке, а вторую под буквами первой в обратном порядке

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

Употребляют в письме верхние буквы вместо нижних и наоборот, а гласные остаются без изменения. Для расшифровки используют тот же способ, что и для шифрования (шифр симметричный).

НАПРИМЕР

Словарь на тарабарской грамоте будет *лсошамь*, великий государь – шеситий чолуцамь.

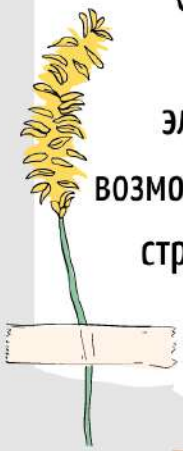
ЗАШИФРУЙТЕ ПОСЛАНИЕ

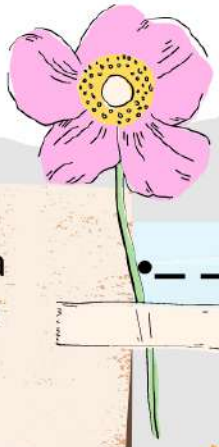
Игорь-князь и Всеволод отважный—
Святослава храбрые сыны —
Вот ведь кто с дружиною бесстрашной
Разбудил поганых для войны!

Азбука Морзе

Способ знакового кодирования, представление букв алфавита, цифр, знаков препинания и других символов последовательностью сигналов: длинных и коротких.

Азбука Морзе используется для облегчения передачи сообщений (с помощью телеграфа). Длинные и короткие сигналы посылаются с помощью включения и выключения электрического тока. Телеграф и азбука Морзе сделали возможной мгновенную передачу информации между разными странами, войсками во время ведения военных действий.





От разведчика была получена следущая зашифрованная радиограмма, переданная с помощью Азбуки Морзе.

•_ _ • • _ • • _ • • • _ _ • • _ • • _ • _ • • _

При передаче радиограммы было потеряно разбиение на буквы, но известно, что в радиограмме использовались только следующие буквы;

А •–	Д –••	Е •	Л •–••
П •––•	Р •–•	Т –	Ь –••–

Пляшущие человечки

Шифр, который вычислил сыщик Шерлок Холмс в одноименном рассказе Артура Конан Дойля. Каждая буква заменяется изображением человечка. Для обозначения конца слова, используется человечек с флагом.

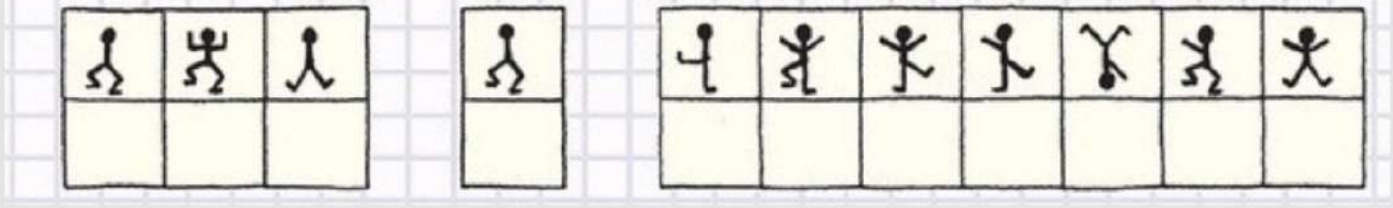
ПРЕИМУЩЕСТВА:

Благодаря стеганографическим свойствам при небольшой длине шифровки может написан где угодно — на заборе, столбе, асфальте и сойдет за детские рисунки.

НЕДОСТАТКИ:

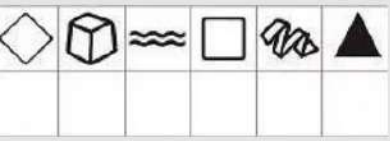
Будучи симметричным шифром простой замены, он не обеспечивает ни достаточной конфиденциальности, ни аутентичности.

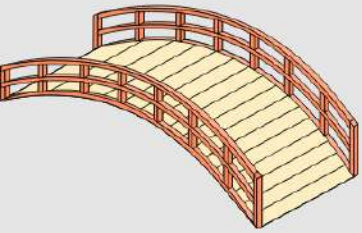
В рассказе английского писателя Артура Конан Дойля знаменитый сыщик Шерлок Холмс разгадывает очередную загадку - в виде пляшущих человечков. Тебе тоже пришло от них послание. С помощью ключа ответь на вопрос: «Что говорят пляшущие человечки?»

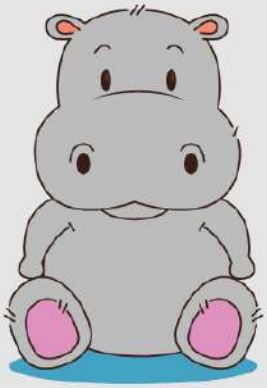


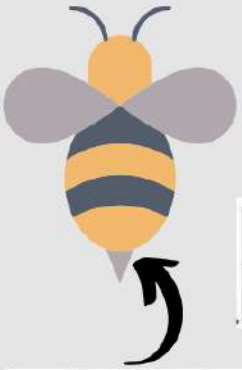
ЗАГАДКА - ШИФРОВКА

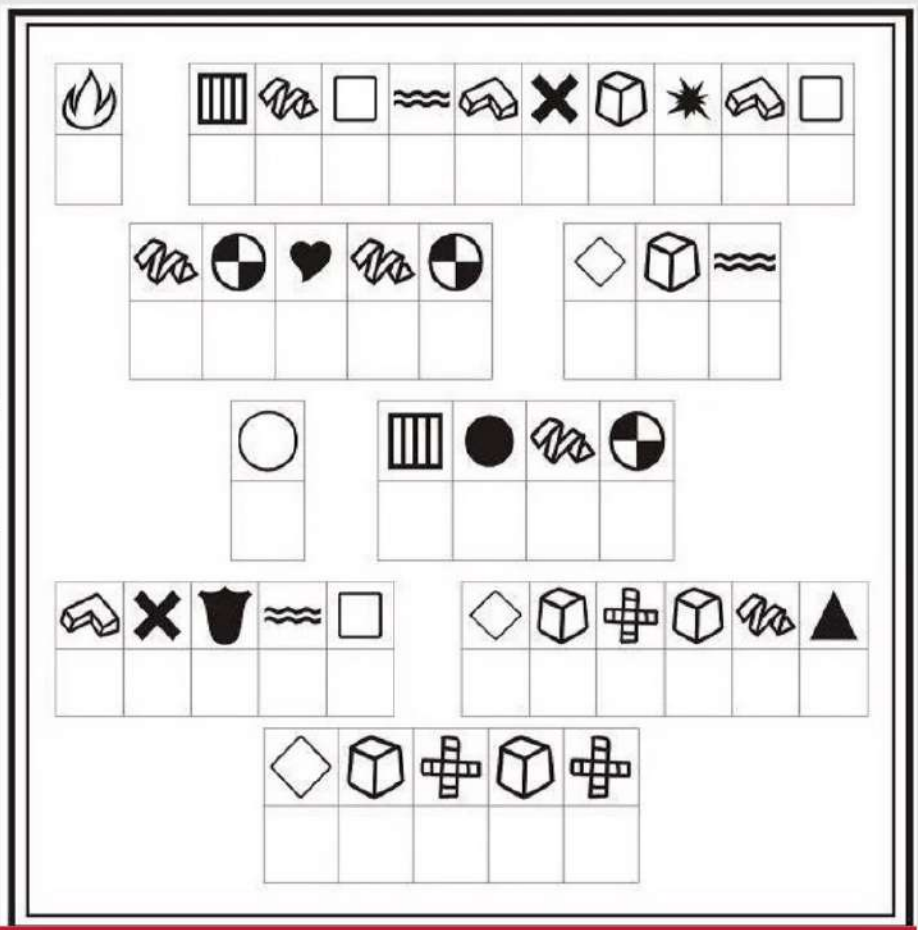
Каждой букве соответсвует свой значок. Подпиши под картинками, что ты на них видишь, а потом заполни саму шифровку, и ты прочитаешь загадку. Отгадай ее.



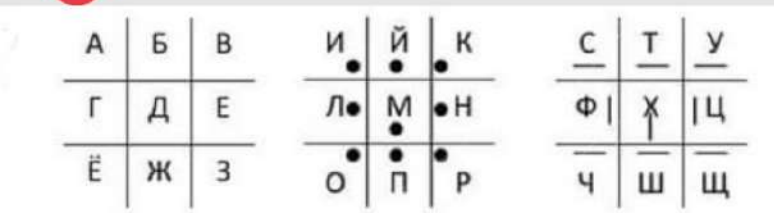








Шифр Pigpen



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

Соедините слова и их шифры

ЛЕС

РАБОТА

ЗИМА

ГЕПАРД

ОЛЕНЬ

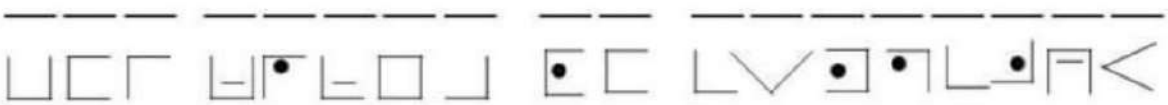
ФРУКТ

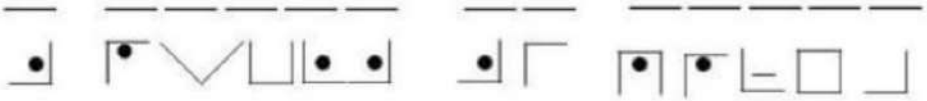
ЁЖ

ВЕЧЕР

ЯМА

Расшифруйте известную русскую пословицу





Предлагаем вам

СОЗДАТЬ СВОЙ УНИКАЛЬНЫЙ ШИФР

Запишите ключ к шифру, способ расшифровки и зашифруйте послание.

Ключ

Способ расшифровки

Послание