Вероятность и шифрование

kaspersky

kaspersky

Подбросим монетку?

http://castlots.org/

kaspersky

Определение вероятности

$$P = \frac{\text{количество благоприятных событий}}{\text{количество всевозможных событий}}$$

“И” $\rightarrow$ “$\cdot$”

“ИЛИ” $\rightarrow$ “ $+$ ”

Задачи для актуализации знаний:

- На клавиатуре телефона 10 цифр, от 0 до 9. Какова вероятность того, что случайно нажатая цифра окажется четной?

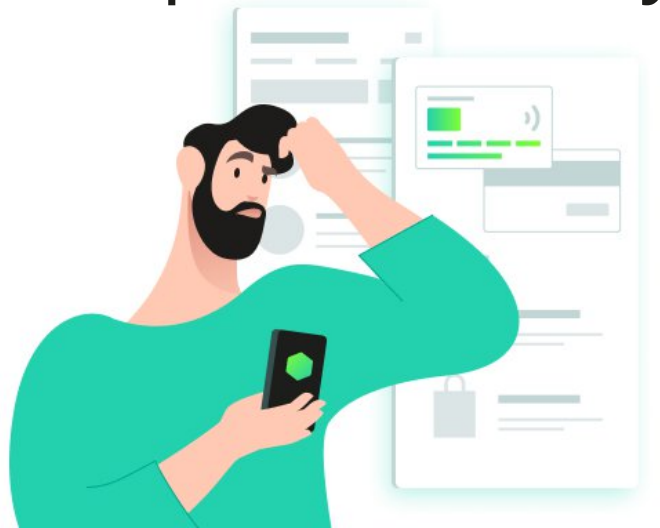
- Рассматриваются символьные последовательности длины 5 в шестибуквенном алфавите {У, Ч, Е, Н, И, К}. Сколько существует таких последовательностей, которые начинаются с буквы У и заканчиваются буквой К?

- Пользователь владеет четырьмя методами шифрования, среди которых – шифр Цезаря. Какова вероятность, что пользователь не воспользуется данным шифрованием?

kaspersky

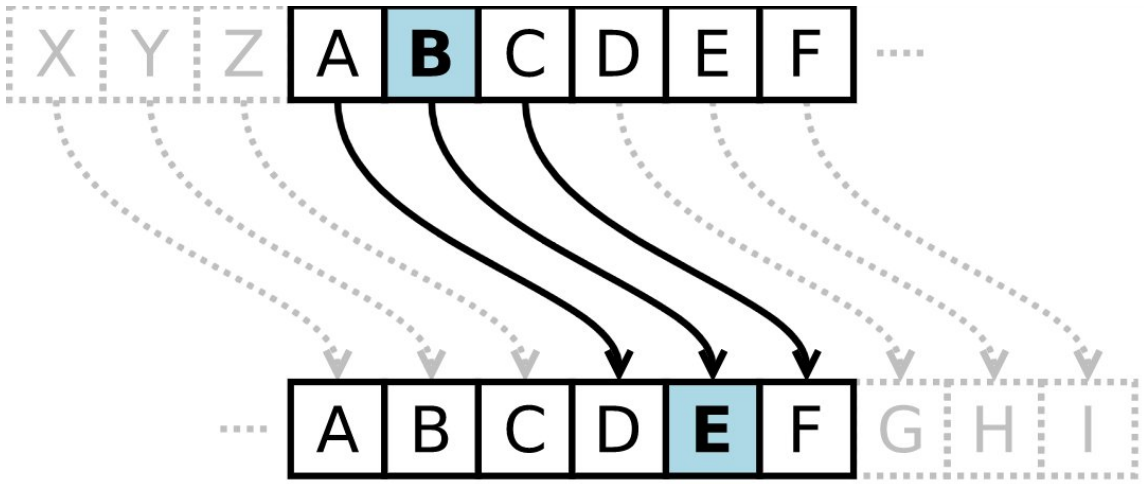
- Для создания пароля из пяти символов пользователь использовал цифры 0, 3, 4, 8 и 9. Какова вероятность подобрать установленный пароль?

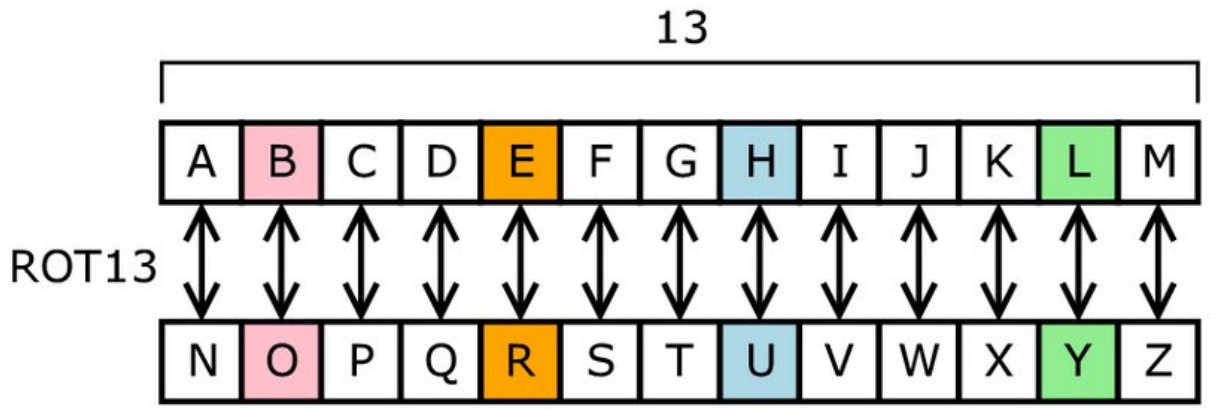
- Вероятность того, что загруженный файл на компьютер с неофициального источника заражен вирусом, равна 0,8. Пользователь загружает два таких файла. Найдите вероятность того, что оба файла окажутся незараженными.

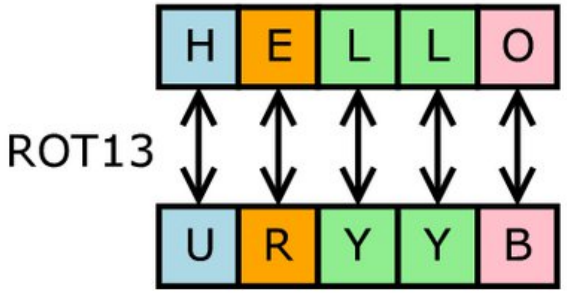


kaspersky

Шифр простой замены







kaspersky

Практическое задание на шифр Цезаря

kaspersky

Расшифруйте фразы:

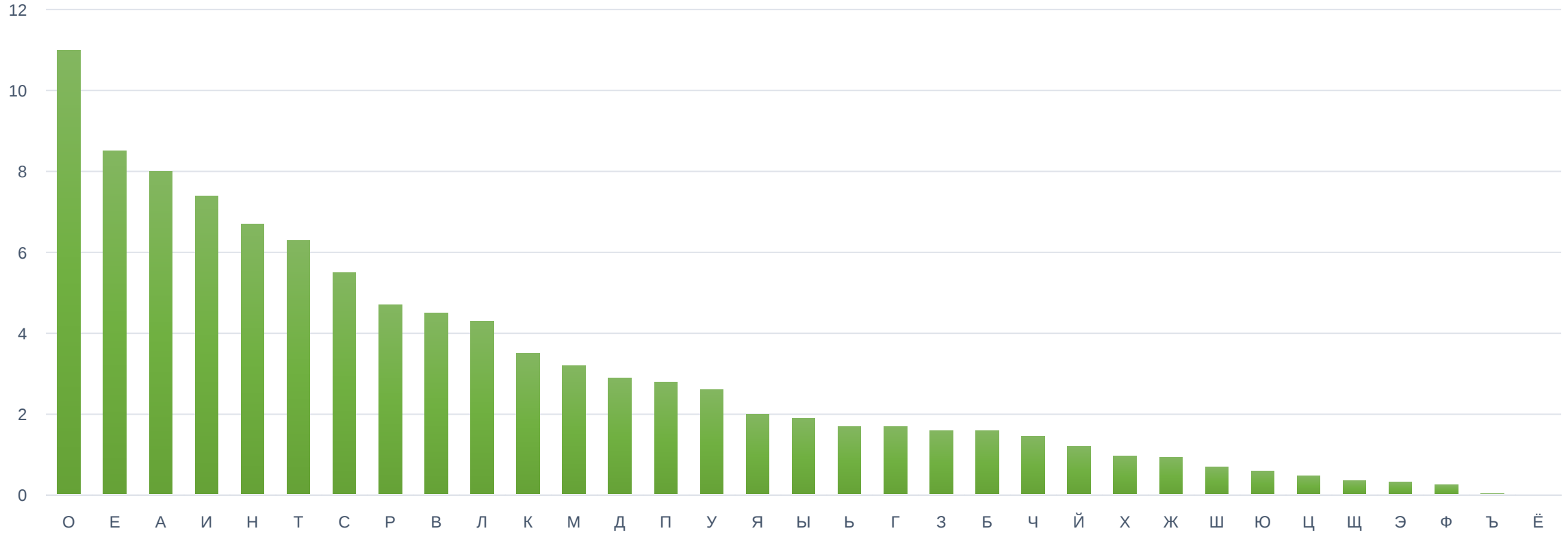
- 1 вариант:
  Тфсфйкь, шб цёчюооъцфзёс!
- 2 вариант: Имкръм, куычюг!
- 3 вариант: Щхюфх япыч Эложчё!

Вопрос:

- Сколько существует возможных перестановок букв русского алфавита?

kaspersky

Частота встречаемости букв русского алфавита



kaspersky

Вопрос:

- В чем плюсы и минусы шифра простой замены?

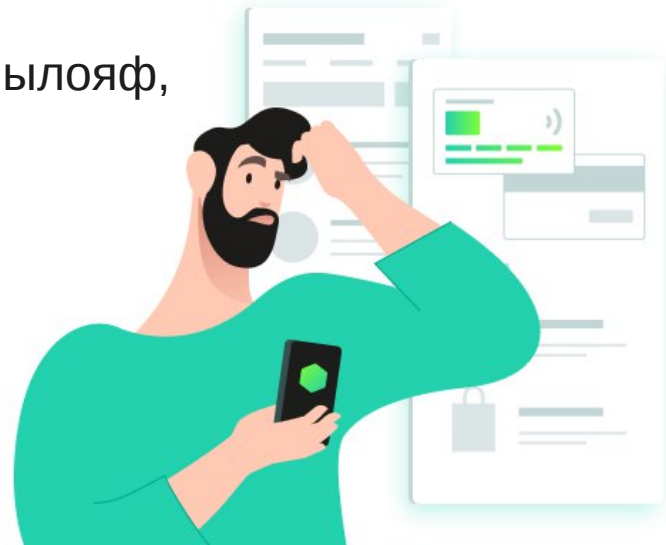
kaspersky

Задание:

- При помощи частотного анализа расшифруйте текст

Тяомджфя ф нмяорнмц нуяюя ьуячятц нмяуя;
Я л убыъх рся нудйяуя,
Змр вмр чур ъёъ съ мяф юругжрх олфц:
Уцжг нмрцм чяэънмц Рзфц.
Рзфрэ н пруыбшцсд нъюъ рся ырнмяуя;
Эъомцм Рзфятц мяф ц наф:
Мр ф мътб цй поцштъм, мр цй ся йэрнм сясцшъм,
Мр цй прсбйяъм, мр цй пруцшъм;
Рзфц съ ыъхнмэлбм сцфяф.
«Мгкл порпянмг! — ьрэроцм рся, — ц мрм ылояф,
Фмр нулжяъм убынфцй энъй эояф:
Энщ пор Рзфц уцжг тсъ сяуьяуц;
Я порфл ся-эрурн съм э сцй».
Тяомджфя млм н ырняыд ц н пъзяуц
Р фятъсг мяф йэямцуя цй,
Змр мругфр юодчьц чянэъофяуц.

- Помощь для анализа: https://planetcalc.ru/733/



kaspersky

Спасибо за внимание!

kaspersky