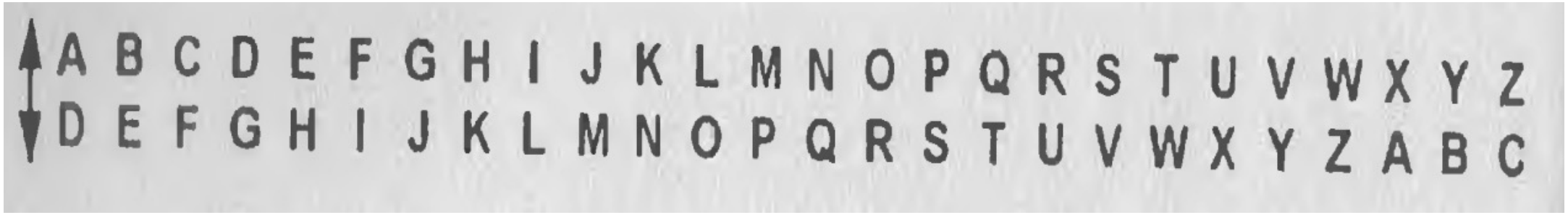
Простейшие шифры

Среди всех шифров можно выделить два больших класса: шифры замены и шифры перестановки. На данном занятии будем рассматривать только шифры замены.

Среди всех шифров можно выделить два больших класса:

- шифры замены
- шифры перестановки

- Шифрами замены называются такие шифры, преобразования в которых приводят к замене каждого символа открытого сообщения на другие символы - шифробозначения, причем порядок следования шифробозначений совпадает с порядком следования соответствующих им символов открытого сообщения.


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

Шифр Цезаря

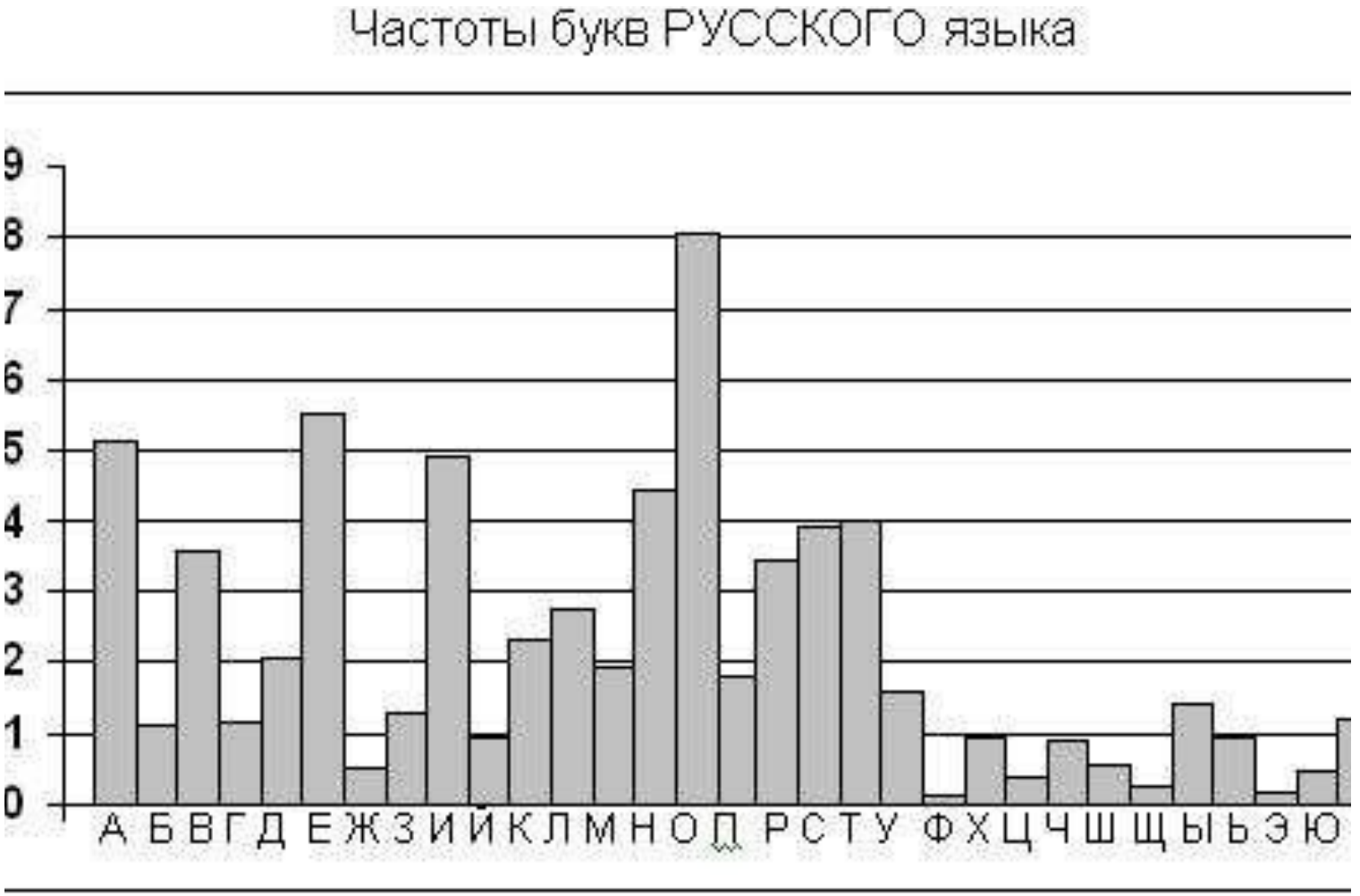
Шифр простой замены

a_1	a_2	a_3	…	a_n
a_{i_1}	a_{i_2}	a_{i_3}	…	a_{i_n}

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	Ы	Ь	Э	Ю	Я
11	98	33	42	19	13	87	54	43	49	48	50	69	32	73	18	81	29	76	74	22	31	90	59	67	77	91	12	52	45

Шифр Полибия

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



Уязвимость шифров вида простой замены

Задача № *2.*

В какое из представленных слов может перейти слово:

B E N E F I T

при использовании сдвигового шифра в английском алфавите?

- WZIZADO;
- SVEWHZK;
- QTCTAXI;
- GJSJKN.

Задача № *4.*

В таблице приведена переписка двух абонентов (Godzillы и Фунтика) в чате.

Фунтик отвечает Godzille и для конспирации каждую букву заменяет другой буквой (при этом разные буквы заменяются разными, а одинаковые - одинаковыми). Восстановите зашифрованное сообщение и пароль

Дата/время	Отправитель	Сообщение
10:11 28.11.2010	Godzilla	Привет. Как дела? Пришли пароль для почты.
10:14 28.11.2010	Фунтик	И усцрмс щюуьсэ ц Яспар-Дюрюмгщмт пс вцю пювючж. Дсмычз: Гщмтщпвжи.
10:21 28.11.2010	Godzilla	Когда доберешься до Питера, позвони.