Криптография

Шифр Цезаря - это вид шифра замены, в котором каждая буква заменяется буквой, находящейся на некотором числе позиций правее неё в алфавите. Например, в шифре со сдвигом на 3, А была бы заменена на Г, Б станет Д, и так далее. Алфавит считается записанным по кругу; так, в приведённом примере буква Ю переходит в Б. Число, на которое мы сдвигаем, называется ключом шифра. Шифр Виженера - усовершенствованный вариант шифра Цезаря. У нас есть ключевое слово, например, БАНК. Мы заменяем каждую его букву на её номер в алфавите: 2 1 15 12. Затем к буквам слова, которое хотим зашифровать, прибавляем по одной числа ключевой последовательности (если она закончилась, начинаем заново). Например, если мы хотим зашифровать слово ГВАРДИЯ, то получим: Г + 2 = Е, В + 1 = Г, А + 15 = О, Р + 12 = Ь, Д + 2 = Ё, И + 1 = Й, Я + 15 = М. Получили ЕГОЬЁЙМ.
Чтобы расшифовать слово ЕГОЬЁЙМ, нужно проводить эти действия в обратном порядке: Е - 2 = Г.

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Задача 1. Расшифруйте слова Гая Юлия Цезаря: ЯОЬ АЭИИЁЬ НЭЕБВИВКЭ КЭ ПНЁ ФЭОПЁ.

Задача 2. Расшифруйте “Фбхй д пудянэрб ёачэ труй рянняшщн!” (ключ: панда, шифр Виженера)

Задача 3. В таблице приведена переписка двух абонентов в чате.

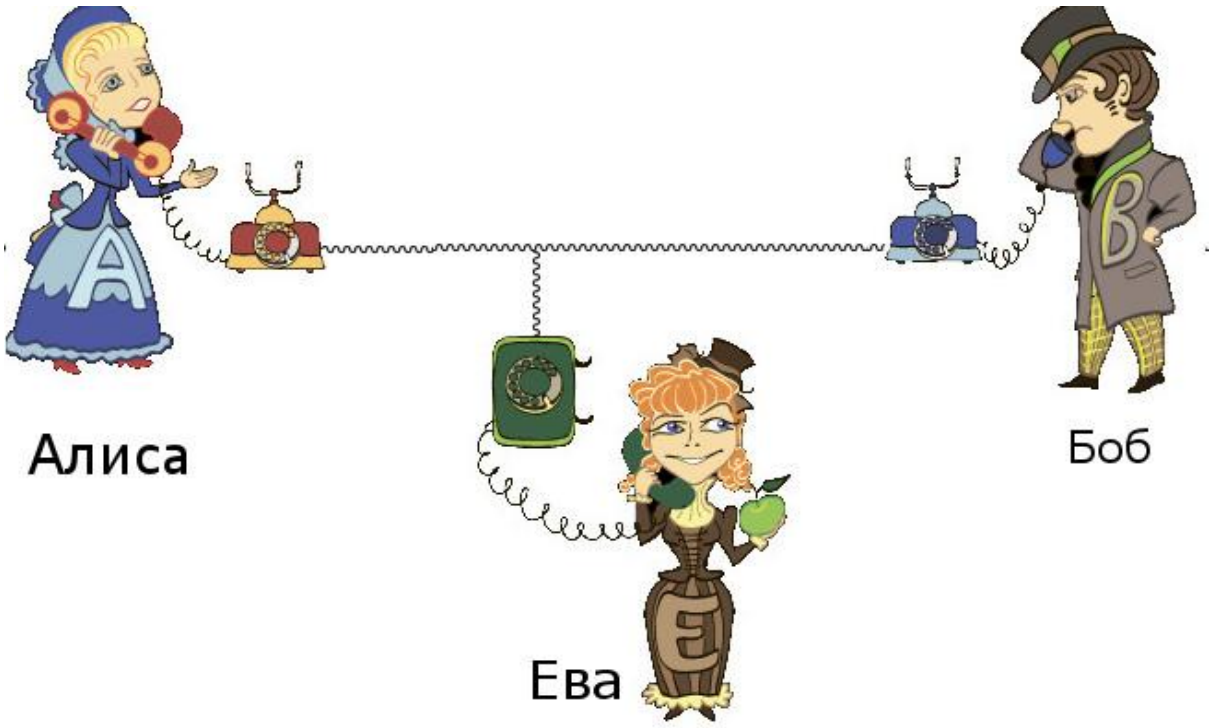
Дата/время	Отправитель	Сообщение
10:11 28.11.2010	Godzilla	**Привет. Как дела? Пришли пароль для почты.**
10:14 28.11.2010	Фунтик	**И усцрмс щюуьсэ ц Яспар-Дюрюмгщмт пс вцю пювючж. Дсмычз: Гщмтщпвжи.**
10:21 28.11.2010	Godzilla	**Когда доберешься до Питера, позвони.**

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

Задача 4. Если слово СРОЧНО зашифровать простой заменой с помощью ключа

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

получится слово ВЗДАБД. Зашифровав полученное слово с помощью того же ключа еще раз, получим ЮШЫЧЯЫ. Сколько всего различных слов можно получить, если указанный процесс шифрования продолжать много-много раз?



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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Криптография еще

Задача 5. Тарабарская грамота
В процессе шифрования гласные остаются на месте, а согласные меняются согласно заранее известному плану (например, на следующую согласную в алфавите).
Попробуйте расшифровать пословицы:
а) Вей фсужа пе гыфабищь и сывлу ий рсужа;
б) Гомлог вояфьтя — г мет пе цожифь;
в) Йпапие — тима.

Задача 6. Сообщение записано в таблицу размера 7×3 слева направо сверху вниз. Затем сверху вниз были выписаны буквы из таблицы: сначала из пятого столбца таблицы, затем из первого, потом из седьмого, второго, четвертого, шестого и третьего: ВАБОЛВЕЫЕКЬТСРТЙЕ.
Что это было за сообщение?

Задача 7. Внимание! В этой задаче в алфавите нет букв ё, й, ъ! Сообщение (из нескольких слов) зашифровано шифром Виженера. Известно, кто ключевая последовательность букв не содержала никаких букв, кроме А, Б и В. Прочтите шифрованное сообщение: РБЬНПТСИТСРРЕЗОХ.

Задача 8. В процессе расследования убийства вы нашли записку преступника, написанную на русском языке, но выглядящую очень странно:
«ЫБЭННЪЪЕРЩЁКЫЙЦЬДЪЫЁЯОЙННМ(В)
ХНЦЗШЧМЪЫИКСУХИЫПЧЪШЧСХНЦСЙЧЙ(Ц)»
Вы знаете, что убийцу зовут Том, ему 31 год, он работает поваром на корабле уже 9 лет (то есть, он — кок), по знаку зодиака он Лев (2-й знак зодиака), а живет он на улице Маков, дом 4. Что же написано в записке?
(Если честно, мы не смогли решить эту задачу :()