Защита информации

В 1997 году Госстандартом России разработан ГОСТ основных терминов и определений в области защиты информации.

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Цифровая информация — информация, хранение, передача и обработка которой осуществляются средствами ИКТ.

Можно различить два основных вида угроз для цифровой информации:

- кража или утечка информации;
- разрушение, уничтожение информации.

Защита информации — деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднаме ренных воздействий на защищаемую информацию.

Несанкционированное воздействие — это преднамеренная порча или уничтожение информации, а также информационного оборудования со стороны лиц, не имеющих на это права (санкции)

Непреднамеренное воздействие происходит вследствие ошибок пользователя, а также из-за сбоев в работе оборудования или программного обеспечения.

Меры защиты информации

- резервное копирование: файлы с наиболее важными данными дублировать и сохранять на внешних носителях;
- осуществлять антивирусную проверку компьютера;
- использовать блок бесперебойного питания.

Цифровая подпись — это индивидуальный секретный шифр, ключ ко торого известен только владельцу.

Цифровой сертификат — это сообщение, подписанное полномочным органом сертификации, который подтверждает, что открытый ключ действительно относится к владельцу подписи и может быть использован для дешифрования.

Практические задания

Шифр Цезаря реализует следующее преобразование текста: каждая буква исходного текста заменяется следующей после нее буквой в алфавите, который считается написанным по кругу.

Используя шифр Цезаря, зашифровать следующие фразы

- Делу время – потехе час

Используя шифр Цезаря, декодировать следующие фразы

- Лмбттоьк шбт

Используя в качестве ключа расположение букв на клавиатуре компьютера, декодировать сообщение

- D ktce hjlbkfcm `kjxrf? D ktce jyf hjckf?

Используя в качестве ключа расположение букв на клавиатуре компьютера, закодируйте сообщение

- Москва – столица России

Шифр перестановки. Кодирование осуществляется перестановкой букв в слове по одному и тому же правилу. Восстановите слова и определите правило перестановки

- НИМАРЕЛ МИНЕРАЛ
- ЛЕТОФЕН ТЕЛЕФОН

Используя шифр перестановки, закодируйте следующие слова:

- **ГОРИЗОНТ** **РОГОЗИТН**
- **ТЕЛЕВИЗОР** **ЛЕТИВЕРОЗ**

Определить правило шифрования и расшифровать слова

КЭРНОЦЛИТКЭЛУОНПИЕЖДАИФЯ

Ответ: Энциклопедия

Используя приведенный нижу ключ, расшифровать сообщение

Ключ: РА ДЕ КИ МО НУ ЛЯ

АКБМУНИЯДКУМВРЛ ИКСЯМТР

Ответ:

РИБОНУКЛЕИНОВАЯ КИСЛОТА

Используя ключ закодировать фразу:

Ключ: РА ДЕ КИ МО НУ ЛЯ

Рыбак рыбака видит издалека

Шифр Виженера. Это шифр Цезаря с переменной величиной сдвига. Величину сдвига задают ключевым словом. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов букв исходного текста: 3 1 9 1 3 1 9 1 и т. д. Используя в качестве ключевого слово ЗИМА, закодировать слова: АЛГОРИТМИЗАЦИЯ

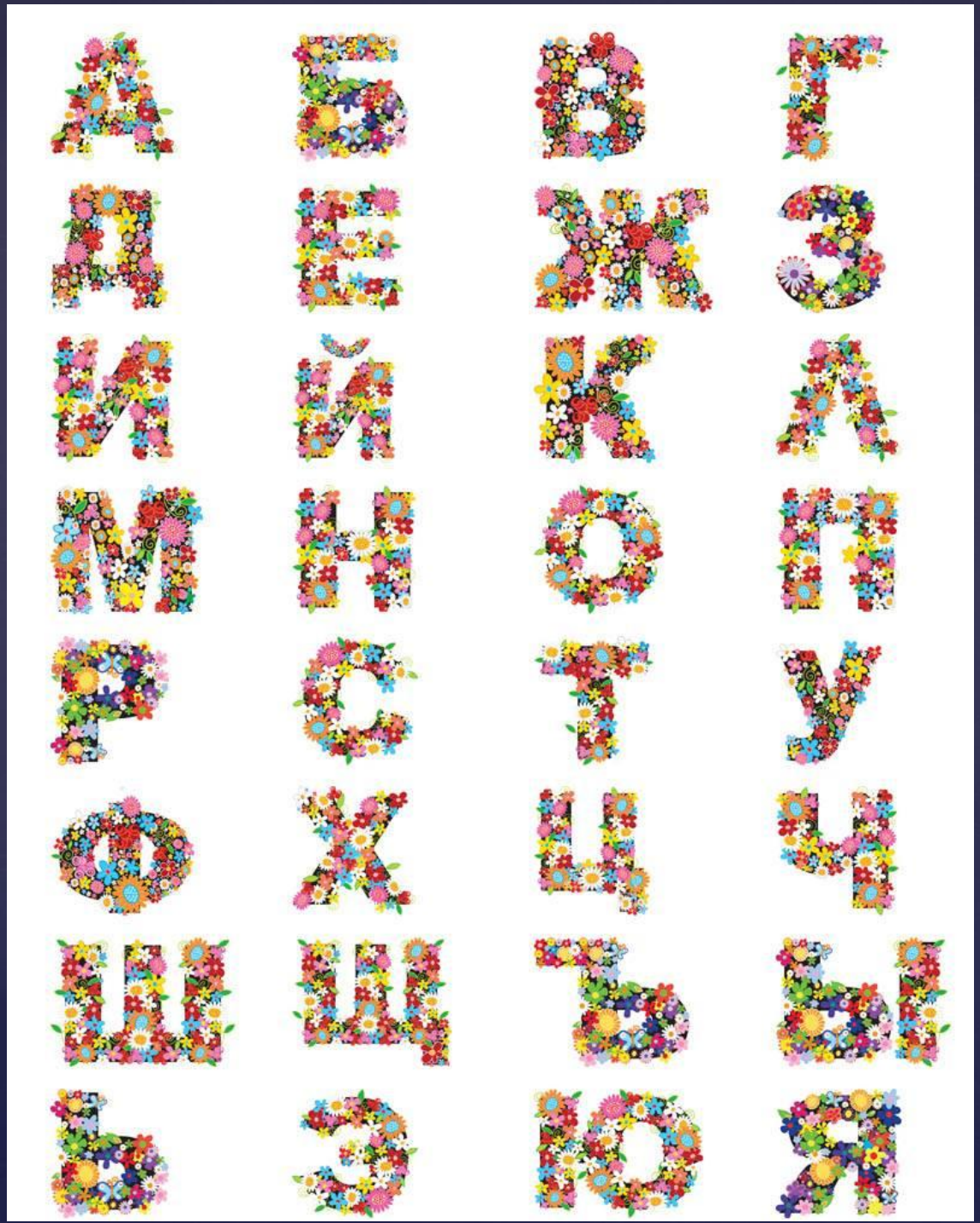
В слове ЗИМА обозначаем буквы их порядковым номером:
З - девятая буква алфавита, И - 10, М - 14, А -1.
Получаем последовательность 9 10 14 1.
ИНТЕРНЕТ.
Букву И сдвигаем на 9 букв, получаем С,
букву Н сдвигаем на 10 букв, получаем Ч
букву Т сдвигаем на 14 букв, получаем А (так как сдвиг на 13 это буква Я, алфавит начинается заново, 14 будет буква А)
букву Е сдвигаем на 1 букву, получаем Ж (если в алфавите Ё не считается)
Букву Р сдвигаем на 9 букв, получаем Щ,
букву Н сдвигаем на 10 букв, получаем Ч
букву Е сдвигаем на 14 букв, получаем У
букву Т сдвигаем на 1 букву, получаем У
ИНТЕРНЕТ = СЧАЖЩЧУУ

Слово ЖПЮЩЕБ получено с помощью шифра Виженера с ключевым словом БАНК. Восстановить исходное слово.

Выпишем алфавит (без ё) и пронумеруем его буквы от 1 до 32
Тогда ЖПЮЩЕБ может быть записано как 7 16 31 26 6 2
Ключ БАНК можно записать как 2 1 14 11.
Запишем номера букв из закодированного слова, а под ними подпишем номера из ключа БАНК нужное количество раз, чтобы количества чисе в обоих строках совпадали.

7 16 31 26 6 2
2 1 14 11 2 1

А теперь вычтем из верхних чисел нижние
5 15 17 15 4 1
Им соответствуют буквы, составляющие слово Д О Р О Г А


А Б В Г
Д Е 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