Шифрование данных с использованием шифра Цезаря, Виженера, перестановки с ключевым словом.

Подготовили студенты
группы 453
Облосов Александр и Мартынов Дмитрий

Шифр

Шифр – совокупность обратимых преобразований множества элементов открытого текста на множество элементов шифротекста, проиндексированных элементами из множества ключей.

Шифрование

Шифрование — обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в **это**же время, авторизованным пользователям доступа к ней. Главным образом, **шифрование** служит задачей соблюдения конфиденциальности передаваемой информации.

Криптоанализ

Криптоанализ - наука (и практика ее применения) о методах и способах вскрытия шифров. Под вскрытием понимается задача получения по известному шифротексту соответствующего открытого текста и/или ключа шифрования.

Криптография

Криптография – наука о методах и средствах преобразования информации в вид, затрудняющий или делающий невозможным несанкционированные операции с нею (чтение и/или модификацию).

Шифр Цезаря

Пример:

Мартынов и Облосов

+10:

Цйъьечшл т Шкхшышл

Шифр Цезаря.Пример

Пример:

Сообщение	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Номер 1	12	18	10	17	20	16	4	18	1	22	10	33
Номер 1 +5	17	23	15	22	25	21	9	23	6	27	15	5
Шифр	П	Х	Н	Ф	Ч	У	З	Х	Е	Щ	Н	Д

Ответ: «Пхнфчузхещнд»

Шифр Цезаря с ключевым словом.

В данной разновидности шифра Цезаря ключ задается числом *k* (0<=*k*<=*n*-1) и коротким ключевым словом или предложением. Выписывается алфавит, а под ним, начиная с *k+1*-й позиции, ключевое слово. Оставшиеся буквы записываются в алфавитном порядке после ключевого слова.

ключевое слово – 'ключ'
k=2

Исходный алфавит	а	б	в	г	д	е	ё	ж	…	э	ю	я
Измененный алфавит	э	я	к	л	ю	ч	а	б	…	ь	ы	ъ

Исходный текст: пример шифрования

Зашифрованный текст: ймгжчм фгрмикэзгъ

Шифр Виженера

Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно.

Шифр Виженера

Ключом шифра служит специальная фраза. Эта фраза, многократно повторяясь,пишется над шифруемым текстом. Каждая буква секретного сообщения получается сдвигом каждой буквы исходного текста на определённое число, задаваемое буквой ключевой фразы (Буква А не даёт сдвига, буква Б — сдвиг на одну позицию, В — на две и т.д.).

Шифр Виженера

Например попробуем зашифровать слово «СЕКРЕТ», пользуясь ключевой фразой «АБВ». Буква С не сдвигается, первая буква Е сдвигается на одну позицию, превращаясь в Ж, буква К сдвигается на две позиции, превращаясь в М. Продолжая шифровать сообщение, мы в итоге получим «СЖМРЖФ».

Шифр перестановки с ключевым словом

Шифр перестановки меняет порядок следования символов.

Простой столбцевой перестановочный шифр

В данном виде шифра текст пишется на горизонтально разграфленном листе бумаги фиксированной ширины, а шифротекст считывается по вертикали. Дешифрирование заключается в записи шифротекста вертикально на листе разграфленной бумаги фиксированной ширины и затем считывании открытого текста горизонтально.

В О Л О Г О
Д С К И Й
Г О С У Д А
Р С Т В Е Н
Н Ы Й П Е
Д А Г О Г И
Ч Е С К И Й
У Н И В Е
Р С И Т Е Т

Зашифрованный текст: ВДГРНДЧ РОСОСЫАЕУСЛКСТЙГСНИООИУВ ОКИТГЙДЕПГИВЕО АНЕИЙЕТ

Перестановочный шифр с ключевым словом

Буквы открытого текста записываются в клетки прямоугольной таблицы по ее строчкам. Буквы ключевого слова пишутся над столбцами и указывают порядок этих столбцов (по возрастанию номеров букв в алфавите). Чтобы получить зашифрованный текст, надо выписывать буквы по столбцам с учетом их нумерации:
Открытый текст: Прикладная математика Ключ: Шифр
Ш и ф р
4 1 3 2
П р и к
л а д н
а я м а
т е м а
т и к а
Криптограмма: Раяеикнаааидммкплатт
Ключевое слово(последовательность столбцов) известно адресату, который легко сможет расшифровать сообщение.