

Кодирование. Шифры

Защита информации

Шифром называют секретный код преобразования информации с целью ее защиты от незаконных пользователей.

Изобретением и использованием шифров занимается **криптография**.



Расшифруйте закодированные слова (кодирование перестановкой)

□ кутлиараав

□ согпррес

□ уткнобу

□ тфорельп

□ нпале

□ шкмаы

□ шистипук

□ шккоа

□ нккооли

□ векаоридта

□ ротмони

□ ккноап

□ килшаав

□ матфоркиина

Азбука Морзе

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

1. Расшифруйте
(декодируйте) выражение
(буквы отделены друг от
друга пробелами):

— — — — — · — · — — — — —
· — · — · — —

2. Закодируйте с помощью
азбуки Морзе слова
АЛГОРИТМ, ШИФР.

Кодировочная таблица

(первая цифра кода – номер строки,
вторая – номер столбца)

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	«				

1. С помощью кодировочной таблицы зашифруйте фразу: Я УМЕЮ РАБОТАТЬ С ШИФРОМ! А ТЫ?
2. Используя кодировочную таблицу, расшифруйте текст:
25201538350304053835111503040038.

Шифр Цезаря

- Этот шифр реализует следующее преобразование текста:

каждая буква исходного текста заменяется третьей после нее буквой в алфавите, который считается написанным по кругу.

1. Используя этот шифр, закодируйте слова КОМПЬЮТЕР, ЧЕЛОВЕК.
2. Расшифруйте слово НУЛТХСЁУГЧЛВ, закодированное с помощью шифра Цезаря.

«Шифры замены»

- Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Шифрование в древние времена

Например, сообщение **НЕЯСНОЕ
СТАНОВИТСЯ ЕЩЕ БОЛЕЕ
НЕПОНЯТНЫМ** записывается в таблицу по столбцам. Для таблицы из 5 строк и 7 столбцов это выглядит так:

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

После того, как открытый текст записан колонками, для образования шифровки он считывается по строкам. Если его записывать группами по 5 букв, то получится: **НОНСБ НЯЕЕО
ЯОЕТА СВЕЛП НСТИЩ
ЕОЫНА ТЕЕНМ.**

Для использования этого шифра отправителю и получателю нужно договориться об общем ключе в виде размера таблицы.

Объединение букв в группы не входит в ключ шифра и используется лишь для удобства записи несмыслового текста.

Домашнее задание

- Закодируйте свое имя и фамилию несколькими видами шифров.