Шифрование данных

Шифрование — это способ изменения сообщения с целью сокрытия его содержимого. В отличие от *кодирования* здесь не существует однозначного соответствия между символами текста и кодом. Для восстановления закодированного сообщения достаточно знать правило замены, а для восстановления зашифрованного сообщения кроме знания правил шифрования требуется еще ***ключ*** к шифру. Знание ключа позволяет ***дешифровать*** текст. Методами ***шифрования*** и ***дешифрования*** занимается наука ***криптография***.

Методы шифрования

Шифр Цезаря - это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется буквой находящейся на некоторое постоянное число позиций левее или правее него в алфавите.
Например, в шифре со сдвигом один вправо:

Символы шифруемого текста	А	Б	В	Г	…	Э	Ю	Я
Заменяющие символы	Я	А	Б	В	…	Ь	Э	Ю

Шифр Виженера – это вид шрифта с переменной величиной сдвига. Величину сдвига задают ключевым словом.
Например, необходимо используя ключевое слово ВАГОН, зашифровать слово АЛГОРИТМ.

Шифрование								
Дано	**А**	**Л**	**Г**	**О**	**Р**	**И**	**Т**	**М**
№ симв	1	13	4	16	18	10	20	14
Сдвиг	3	1	4	16	15	3	1	4
№ симв. замены.	4	14	8	32	33	13	21	18
Шифр	**Г**	**М**	**Ж**	**Ю**	**Я**	**Л**	**У**	**Р**

Ключ				
В	**А**	**Г**	**О**	**Н**
3	1	4	16	15

Домашнее задание «Шифрование данных»
Задание 1

	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	:	;	-	!	»				

Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

а) С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ РАБОТАТЬ С ИНФОРМАЦИЕЙ! А ТЫ?
б) Используя кодировочную таблицу, расшифруйте текст: 252015383503040538351115030400 38

Задание 2
Используя ключевое слово ВАГОН, зашифруйте слова ПРАВИЛА и ИНФОРМАЦИЯ с помощью шрифта Виженера.