ШИФРОВАНИЕ И ДЕШИФРОВАНИЕ

Выполнила: Васильева Сардаана Николаевна

Студентка гр.ПКС-15

Что такое шифрование и дешифрование?

- **Шифроваание** – это обратимое преобразование информации в целях скрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма

- **Дешифрование** – это анализ документа, написанного на неизвестном языке и/или неизвестной системой письма. Чаще всего термин используется по отношению к прочтению древних документов.
- О шифровании сообщений и соответствующих математических методах см. статью Криптография. Следует заметить, что в криптографии термины «дешифрование» и «расшифрование» имеют различный смысл

Метод шифрования АТБАШ

Простой шифр подстановки для алфавитного письма. Правила шифрования состоит в замене i-ной буквы алфавита буквой с номером n-i+1 где n-число букв в алфавите. Ниже даны примеры для латинского и еврейского алфавита:

Исходный текст	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Зашифрованный текст	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Исходный текст	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
Зашифрованный текст	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

Один из наиболее простых способов шифрования. Первая буква алфавита заменяется на последнюю, вторая – на предпоследнюю и т.д.
Пример: « SCIENCE » = HXRVMXV

8. Шифр Атбаш

Древний шифр, использовавшийся иудеями для шифрования священных текстов.

В основе, которого лежит ***метод замены***: вместо *первой буквы* алфавита писалась *последняя* буква, вместо второй - предпоследняя т.д.

А	Я
Б	Ю
В	Э
Г	Ь

Д	Ы
Е	Ъ
Ж	Щ
З	Ш

И	Ч
Й	Ц
К	Х
Л	Ф

М	У
Н	Т
О	С
П	Р

Например: То= З А К Р О Й Д В Е Р Ь

Расшифрование: Ч Я Ф О Р Х Ы Э Ъ О Г

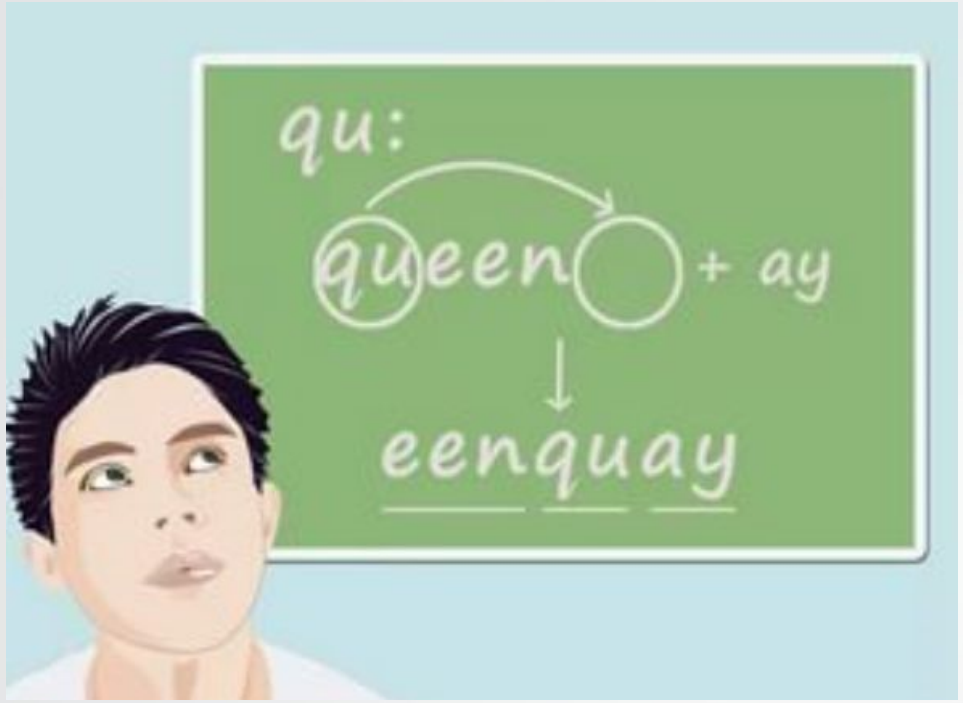
Дешифрование: З А К Р О Й Д В Е Р Ь

Метод шифрования и дешифрования «Поросячья латынь»

«Тайный язык», представляющий собой зашифрованный английский. Чаще всего используется в шутливом или полушутливом контексте. В Великобритании также называется *backslang*.

Вопреки своему названию, поросячья латынь никак не связана с настоящей. «Перевод» с английского языка осуществляется следующим образом.

1. Если слово начинается на один или несколько согласных звуков, первые согласные перемещаются в конец слова и добавляется *ay*. Так *ball* («шар», «мяч») превращается в *all-bay*, *button* («пуговица», «кнопка») — в *utton-bay*, *star* («звезда») — в *ar-stay*, *three* («три») — в *ee-thray*, *question* («вопрос») — в *estion-quay*.
2. Если слово начинается на гласный звук, в конце просто добавляется определённый слог, оканчивающийся на *ay*. Какой именно слог, зависит от конкретного «диалекта» поросячьей латыни: это могут быть слоги *way*, *yay*, *hay*, а чаще просто *ay*. Таким образом, *a* (неопределённый артикль) в зависимости от «диалекта» превращается в *a-ay*, *a-way*, *a-yay* или *a-hay*. Следует иметь в виду, что, напр. *honest* («честный») переводится как *honest-ay*, а не *onest-hay*, так как это слово начинается на *согласную букву*, но на *гласный звук*, первая буква *h* не произносится.
3. Если слово оканчивается на «е» немое, то оно может отбрасываться, а может и нет — это зависит от конкретного диалекта поросячьей латыни.



На русский язык мы на согласных возьмем «тар», а на гласных «пэй».

Пример на согласных: То= «Ложись на кровать»
Шифрование: «Ожись – лтар а-нтар овать-кртар»
Дешифрование: «Ложись на кровать».
Пример для гласных: То= «Открой окно»
Шифрование: «Открой – пэй окно - пэй »