Шифр простой замены

Милёхин Александр НПМмд-02-21

Цель лабораторной работы

Изучение шифрования методом простой замены

Криптография

Криптография (от греч. *тайное письмо*) — наука о математических методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.
В древности криптография вызывала огромный интерес, так как позволяла безопасно передавать информацию.

Шифр Цезаря

Шифр Цезаря, также известный, как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования. Он является моноалфавитным, то есть имеет подстановочный тип, где каждая буква в открытом тексте заменяется на другую букву, смещенную на определенное количество позиций в алфавите.
Шифр Цезаря называется так благодаря Юлию Цезарю, который использовал его со сдвигом 3, чтобы защищать военные сообщения. Не смотря на то, что Цезарь считается первым зафиксированным человеком, использующим эту схему, другие шифры подстановки, как известно, использовались и раньше.
Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Пример шифрования со сдвигом 5

Сообщение	**К**	**Р**	**И**	**П**	**Т**	**О**	**Г**	**Р**	**А**	**Ф**	**И**	**Я**
Номер п/п	12	18	10	17	20	16	4	18	1	22	10	33
Номер п/п +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

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике. Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

$$y = (x + k) \bmod n$$
$$x = (y - k + n) \bmod n$$

где: *x* — символ открытого текста, *y* — символ шифрованного текста, *n* — мощность алфавита, *k* — ключ.

Шифр Атбаш

Самым простым способом шифрования является замена одних символов другими: обычно кодирование происходит в рамках одного алфавита, однако могут использоваться и системы разных языков.

Частный случай такого шифрования — шифр простой замены Атбаш. Он использовался для еврейского алфавита и оттуда же получил свое название. Его название составлено из букв алфавита: алеф, таб, бет и шин, которые переставлены местами. Этот шифр возник примерно 3000 лет назад и применялся ессеями: обособленным еврейским сообществом, закрытым орденом, покинувшим большие города в поисках духовной чистоты.

Ключ к расшифровке Атбаш прост: первая буква алфавита должна быть заменена на последнюю, вторая – на предпоследнюю и так до последней буквы, которая станет первой. На языке математики эту замену можно представить в с такой формуле: $i = n - j + 1$,

где j – это номер символа, который мы хотим зашифровать, а n – количество всех символов алфавита.

Шифр Атбаш для английского алфавита:

Исходный алфавит	**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**
Алфавит замены:	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

Результаты выполнения лабораторной работы

Я освоил шифрование методом простой замены и реализовал программу для шифрования на языке Python.

Спасибо за внимание