Методы шифрования

Выполнил: Шелин Илья Ярославович
Проверил: Кулаченков Кирилл Вадимович

Постановка задачи

Зашифровать осмысленный текст высокой важности. Шифрование и дешифрование выполнять с использованием зашифрованного ключа. Шифрование ключа выполнять множеством математических операций с обратимостью.
Задача должна быть реализована как законченное приложение со скрытыми формулами и открытыми полями ввода

Средства реализации

Для реализации поставленной задачи мной была использована программаMicrosoft Excel

Основные понятия

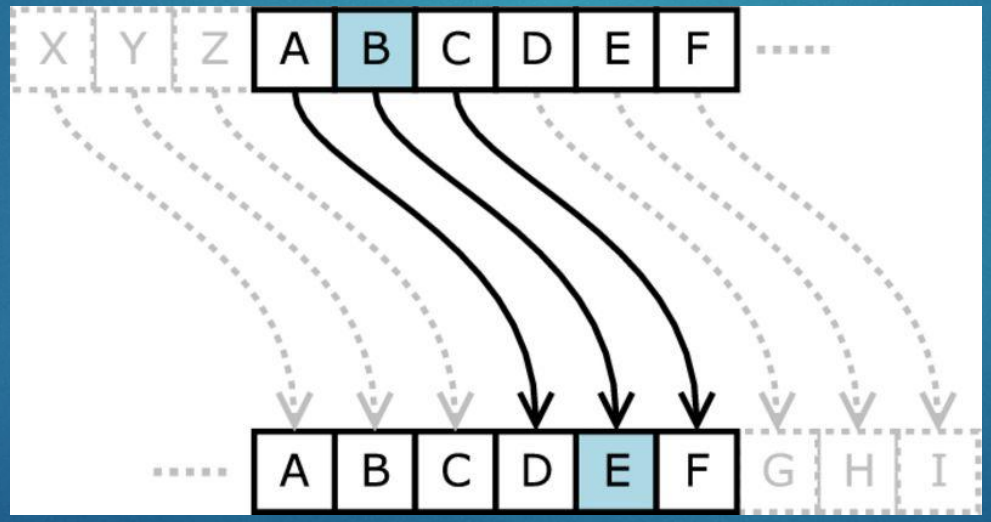
Шифрование - обратимое преобразование информации в целях ограничения доступа посторонних лиц к информации.

Шифр - совокупность методов и способов обратимого преобразования информации с целью ее защиты от несанкционированного доступа (обеспечения конфиденциальности информации).

Ключ - это секретная информация, используемая криптографическим алгоритмом при шифровании/дешифровании информации. При использовании одного и того же алгоритма результат шифрования зависит от ключа.

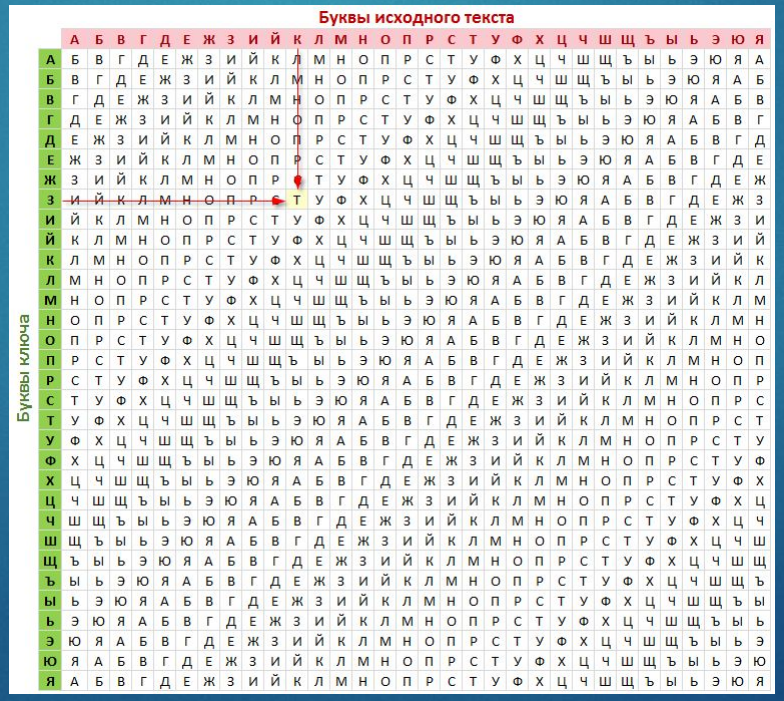
Методы шифрования. Метод Цезаря

При шифровании методом Цезаря буквы исходного текста смещаются на N позиций в алфавитном порядке.



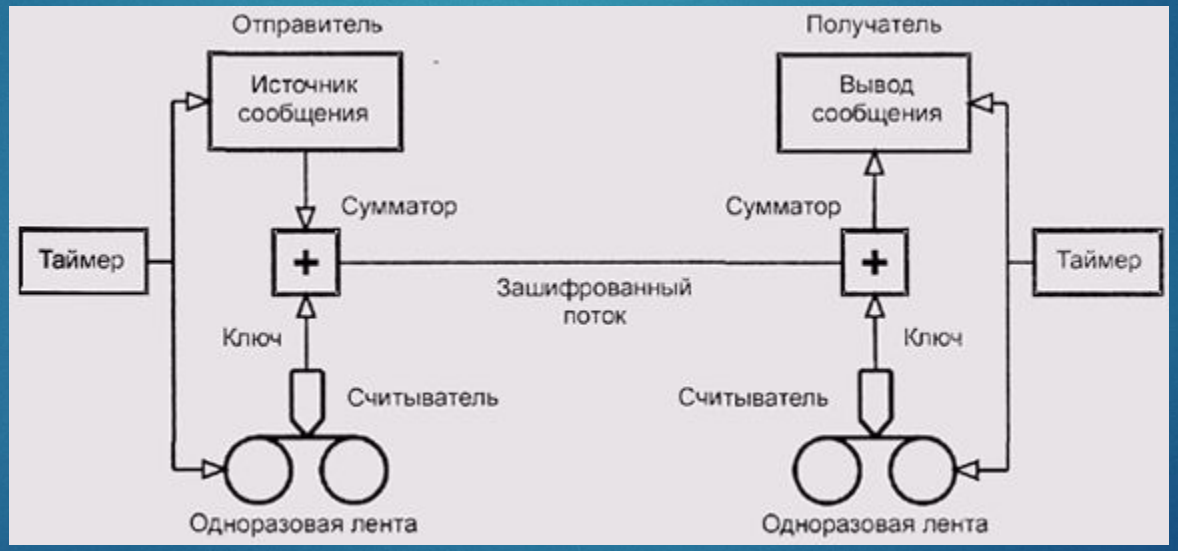
Методы шифрования. Метод Виженера

Этот Шифр многоалфавитной замены можно описать таблицей шифрования. Каждая строка таблицы представляет собой символы используемого алфавита с циклическим сдвигом на n позиций.



Методы шифрования. Метод Вермана

Метод Вернама использует двоичное представление символов исходного текста



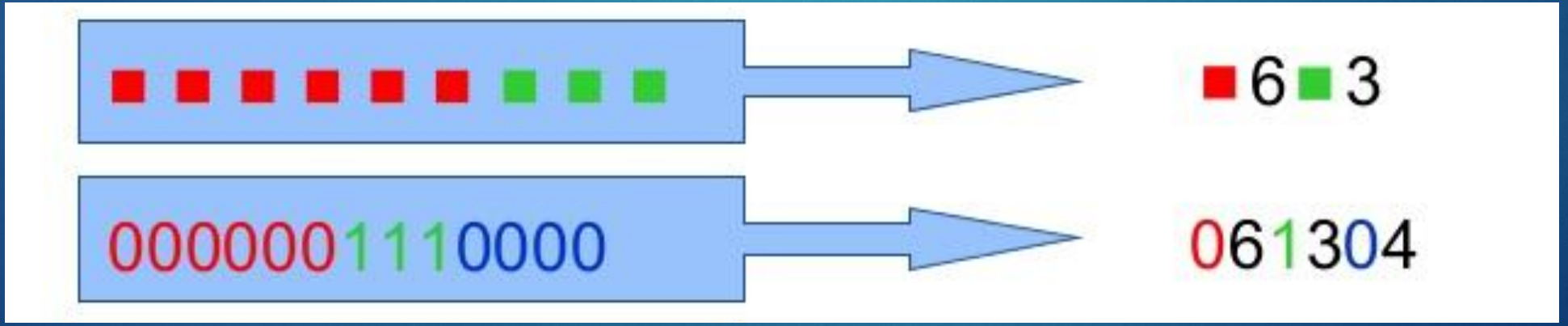
Методы шифрования. Метод Плейфера

Шифр Плейфера использует матрицу 6x6, содержащую ключевое слово или фразу. Ключевое слово, дополненное алфавитом составляет матрицу и является ключом шифра.

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	-	-	-

Методы шифрования. Алгоритм шифрования RLE

RLE (англ. run-length encoding) - Кодирование длин серий. Шифр используется для сжатия информации путём сведения одинаковых элементов. Применяется в основном в шифровании (кодировании) изображений.



Методы шифрования. Метод Гронсфельда

Этот шифр сложной замены, называемый шифром Гронсфельда, представляет собой модификацию шифра Цезаря с числовым ключом.

Сообщение	В	О	С	Т	О	Ч	Н	Ы	Й	Э	К	С	П	Р	Е	С	С
Ключ	2	7	1	8	2	7	1	8	2	7	1	8	2	7	1	8	2
Шифртекст	Д	Х	Т	Ь	Р	Ю	О	Г	Л	Д	Л	Щ	С	Ч	Ж	Щ	У

Методы шифрования. Метод Полибия

К каждому языку отдельно составляется таблица шифрования с одинаковым (не обязательно) количеством пронумерованных строк и столбцов, параметры которой зависят от его мощности (количества букв в алфавите).

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Сравнение методов шифрования

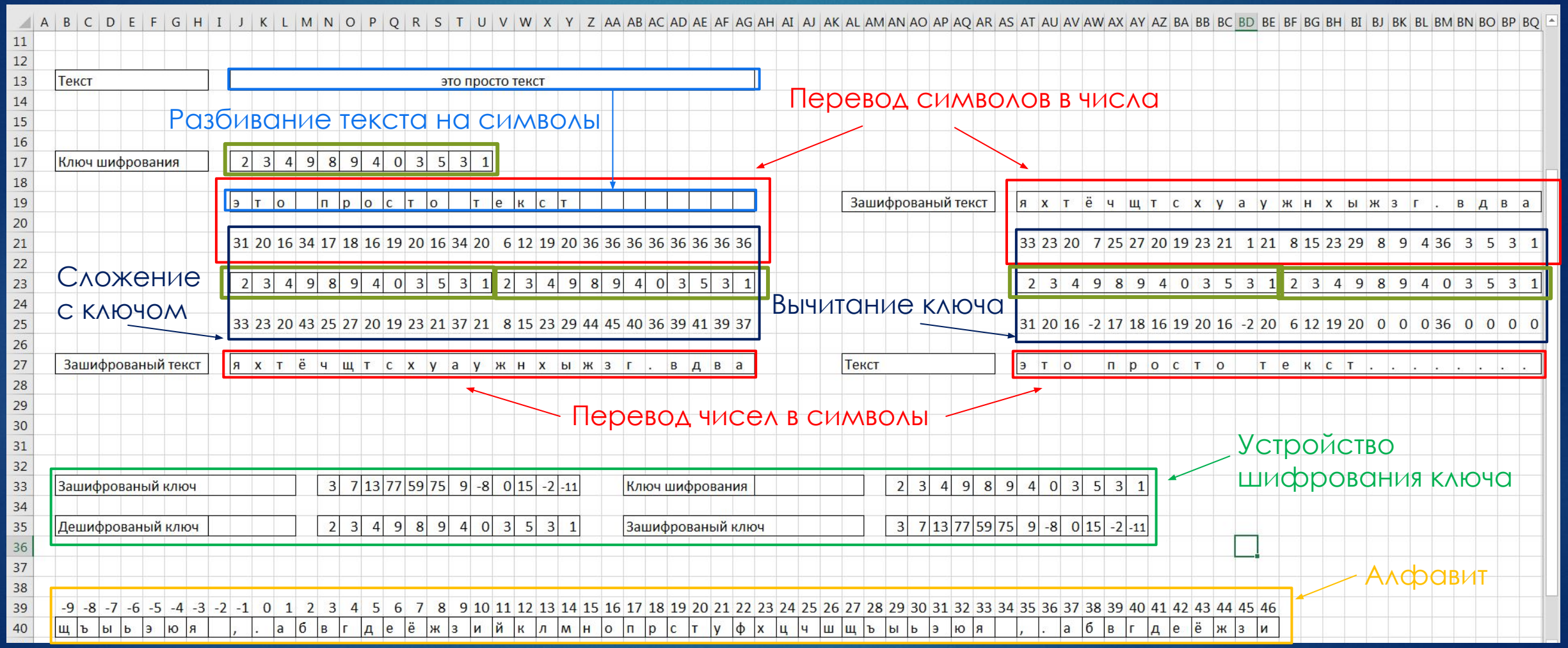
	Наличие ключа шифрования	Надёжность	Наличие матрицы	Простота реализации	Размер ключа
Шифр Цезаря	+\-	Низкая	-	Очень просто	Очень маленький
Шифр Виженера	+	Высокая	-	Просто	Большой
Шифр Вернама	+	Средняя	-	Просто	Большой
Шифр Плейфера	+	Высокая	+	Сложно	Средний
Шифр RLE	-	Низкая	-	Очень просто	-
Шифр Гронсфельда	+	Высокая	-	Нормально	Любой
Шифр Полибия	+	Высокая	+	Сложно	Средний

Метод Гронсфельда

- Матрица отсутствует;
- есть ключ шифрования;
- возможность проведения математических операций с ключом шифрования.

Как было сказано выше, метод Гронсфельда является шифром сложной замены, основанный на шифре Цезаря. Главным отличием данного шифра от шифра Цезаря в количестве операций, а как следствие, и в более высокой надёжности. Для шифрования текста методом Гронсфельда каждая буква смещается на N позиций по алфавиту (N-разряд ключа шифрования).

Реализация


Текст
это просто текст
Разбивание текста на символы
Перевод символов в числа
Ключ шифрования
2 3 4 9 8 9 4 0 3 5 3 1
э т о п р о с т о т е к с т
31 20 16 34 17 18 16 19 20 16 34 20 6 12 19 20 36 36 36 36 36 36 36 36
Зашифрованый текст
я х т ё ч щ т с х у а у ж н х ы ж з г . в д в а
33 23 20 7 25 27 20 19 23 21 1 21 8 15 23 29 8 9 4 36 3 5 3 1
Сложение с ключом
2 3 4 9 8 9 4 0 3 5 3 1 2 3 4 9 8 9 4 0 3 5 3 1
33 23 20 43 25 27 20 19 23 21 37 21 8 15 23 29 44 45 40 36 39 41 39 37
Вычитание ключа
2 3 4 9 8 9 4 0 3 5 3 1 2 3 4 9 8 9 4 0 3 5 3 1
31 20 16 -2 17 18 16 19 20 16 -2 20 6 12 19 20 0 0 0 36 0 0 0 0
Зашифрованый текст
я х т ё ч щ т с х у а у ж н х ы ж з г . в д в а
Текст
э т о п р о с т о т е к с т . . . . . .
Перевод чисел в символы
Устройство шифрования ключа
Зашифрованый ключ
3 7 13 77 59 75 9 -8 0 15 -2 -11
Ключ шифрования
2 3 4 9 8 9 4 0 3 5 3 1
Дешифрованый ключ
2 3 4 9 8 9 4 0 3 5 3 1
Зашифрованый ключ
3 7 13 77 59 75 9 -8 0 15 -2 -11
Алфавит
-9 -8 -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46
щ ъ ы ь э ю я , . а б в г д е ё ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я , . а б в г д е ё ж з и

Вывод

На основании изученных материалов по выявленным методам шифрования текста, сравнения изученных методов и составления сводной таблицы было выяснено , что для реализации поставленной задачи лучше всего подходит шифр Гронсфельда.
Во время выполнения практической работы мной были получены знания об основных методах шифрования и их применения

Спасибо за внимание