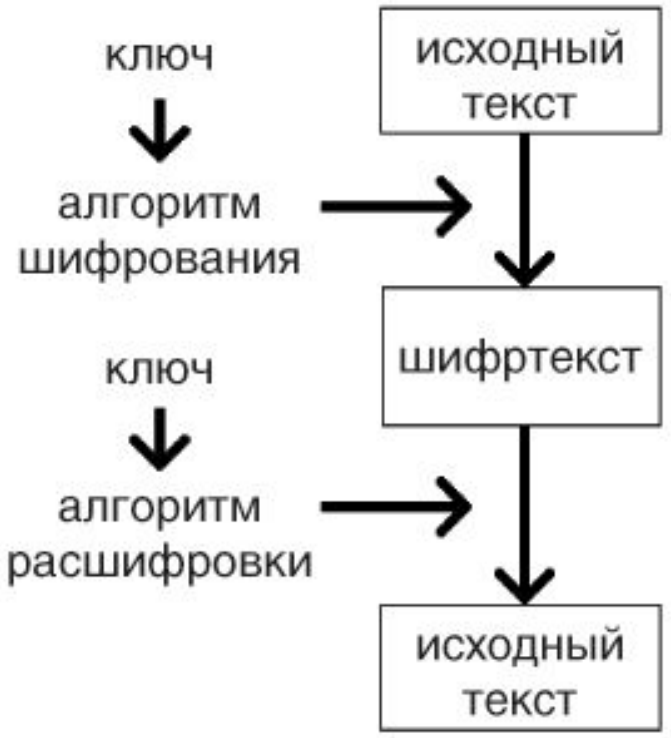
Классическая криптография и кодирование
(Crypto and encoding)

Немного теории. Шифрование vs Кодирование

Шифрование — это способ изменения сообщения или другого документа, обеспечивающее искажение (сокрытие) его содержимого.

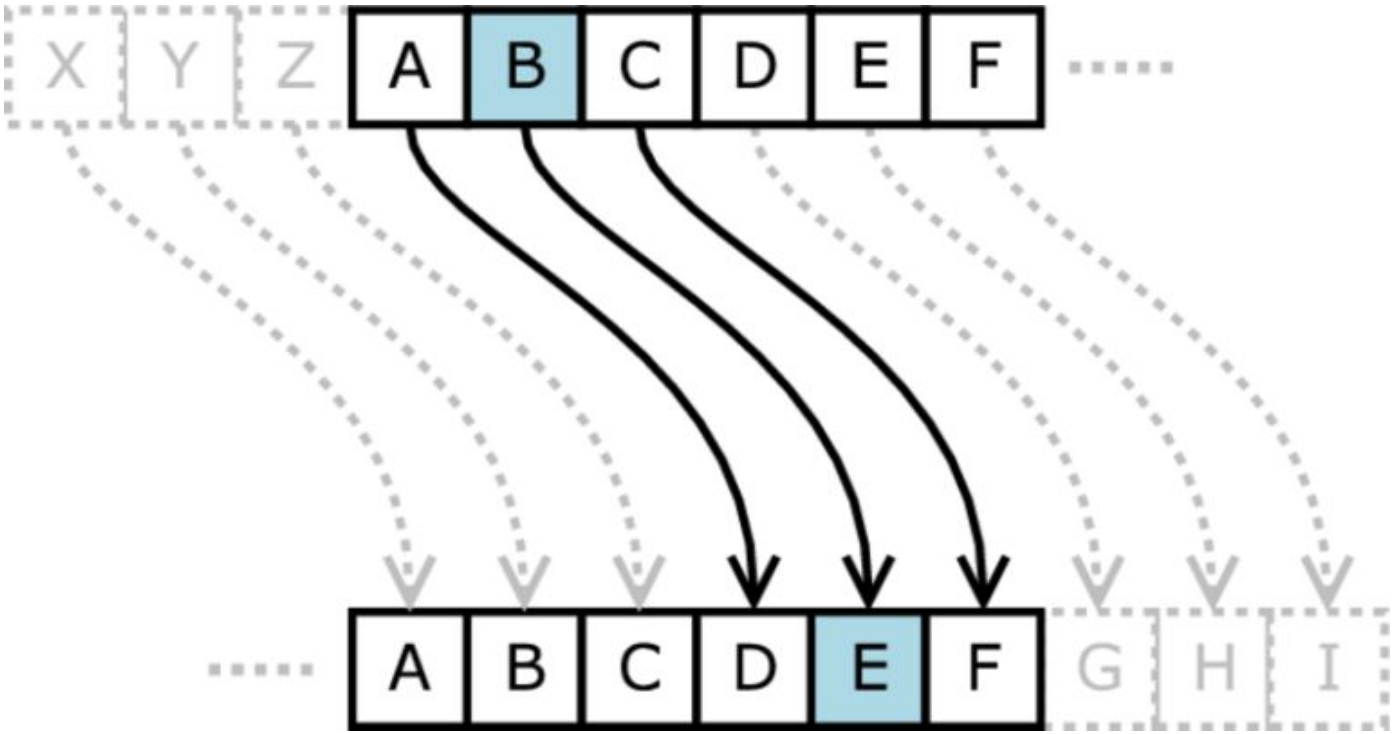
Кодирование – это преобразование обычного, понятного, текста в код. При этом подразумевается, что существует взаимно однозначное соответствие между символами текста (данных, чисел, слов) и символьного кода – в этом принципиальное отличие кодирования от шифрования.



Классические шифры

Шифр Цезаря

Шифр Цезаря один из наиболее древнейших известных шифров. Схема шифрования очень проста — используется сдвиг буквы алфавита на фиксированное число позиций. Используемое преобразование обычно обозначают как ROTN, где N — сдвиг, ROT — сокращение от слова ROTATE, в данном случае «циклический сдвиг».



Пример

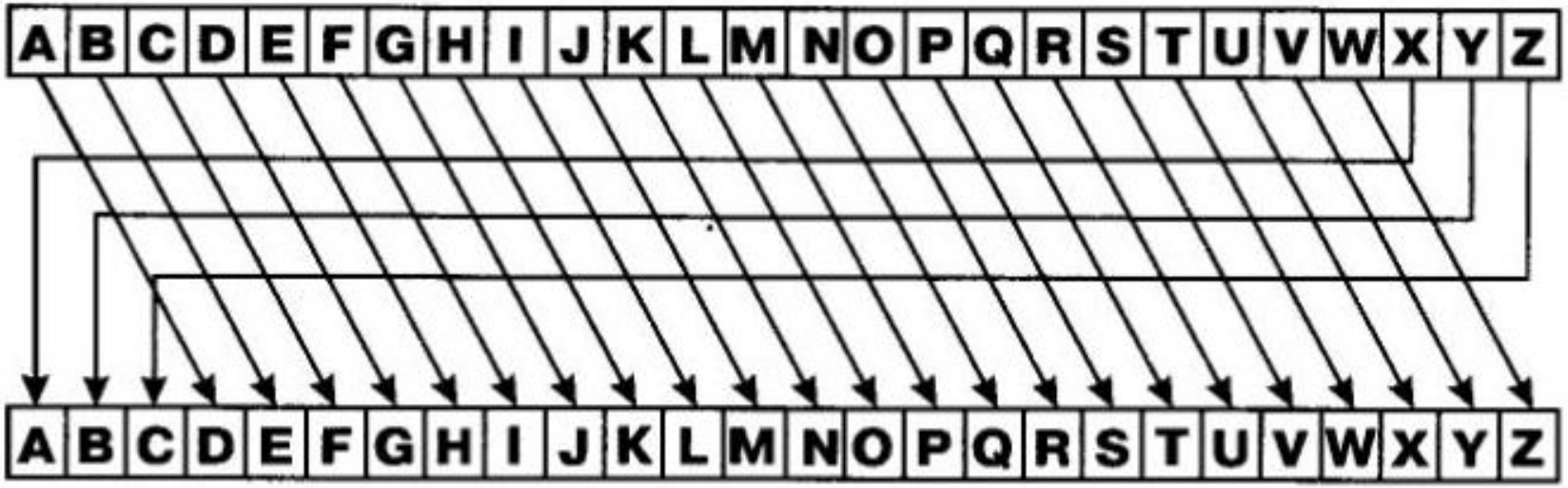


Рис. 2.3. Шифр Цезаря

Ключ: 3

Открытый текст:

P = HELLO CAESAR CIPHER

Зашифрованный текст:

C = KHOOR FDHVDU FLSKHU

Пример

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

Пример

Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З». Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее.
Исходный алфавит:АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
Шифрованный: ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ

Шифр Скитала

Скитала (или ***сцитала*** — от греческого, жезл) — инструмент, используемый для осуществления перестановочного шифрования, в криптографии известный также как **шифр Древней Спарты**. Представляет собой цилиндр и узкую полоску пергамента, на которой писалось сообщение, обматывавшуюся вокруг него по спирали. Античные греки и спартанцы, предположительно, использовали этот шифр для обмена сообщениями во время военных кампаний.

Пример

Пусть есть какой-нибудь текст, например, **НАС_АТАКУЮТ**. Его нужно выписать в табличку размерами ***m*** строк и ***n*** *столбцов*. Размеры подбираются так, чтобы при записи одного символа в одну ячейку весь текст влез в эту таблицу.

По-другому нельзя - здесь нет разбиения текста на блоки, как, скажем, это делается в методе простых шифрующих таблиц. В принципе возможны случаи, когда останутся незанятые ячейки, например, если количество символов в тексте - простое число. Такие ячейки заполняются пробелом или другим заранее выбранным символом.

Текст выписывается вот как:

Н	А	С	_
А	Т	А	К
У	Ю	Т	_

Пример

Н	А	С	_
А	Т	А	К
У	Ю	Т	_

Первые ***n*** символов выписываются в первую строку слева направо (в примере *n*=4, *m*=3). Следующие символы выписывается во вторую строку, пока она не заполнится. И так далее. Если все символы выписаны, а остались незаполненные ячейки, то они заполняются пробелом. Если выписаны не все символы, а таблица заполнена, значит, при выборе размеров допущена ошибка.

Далее производится считывание по столбцам. Сначала по самому левому сверху вниз, затем по его правому соседу также сверху вниз и т.д. В этом случае получится **НАУАТЮСАТ _К_.** Как видно, символы, которые забиты в "лишние" ячейки (пробел), не выбрасываются.

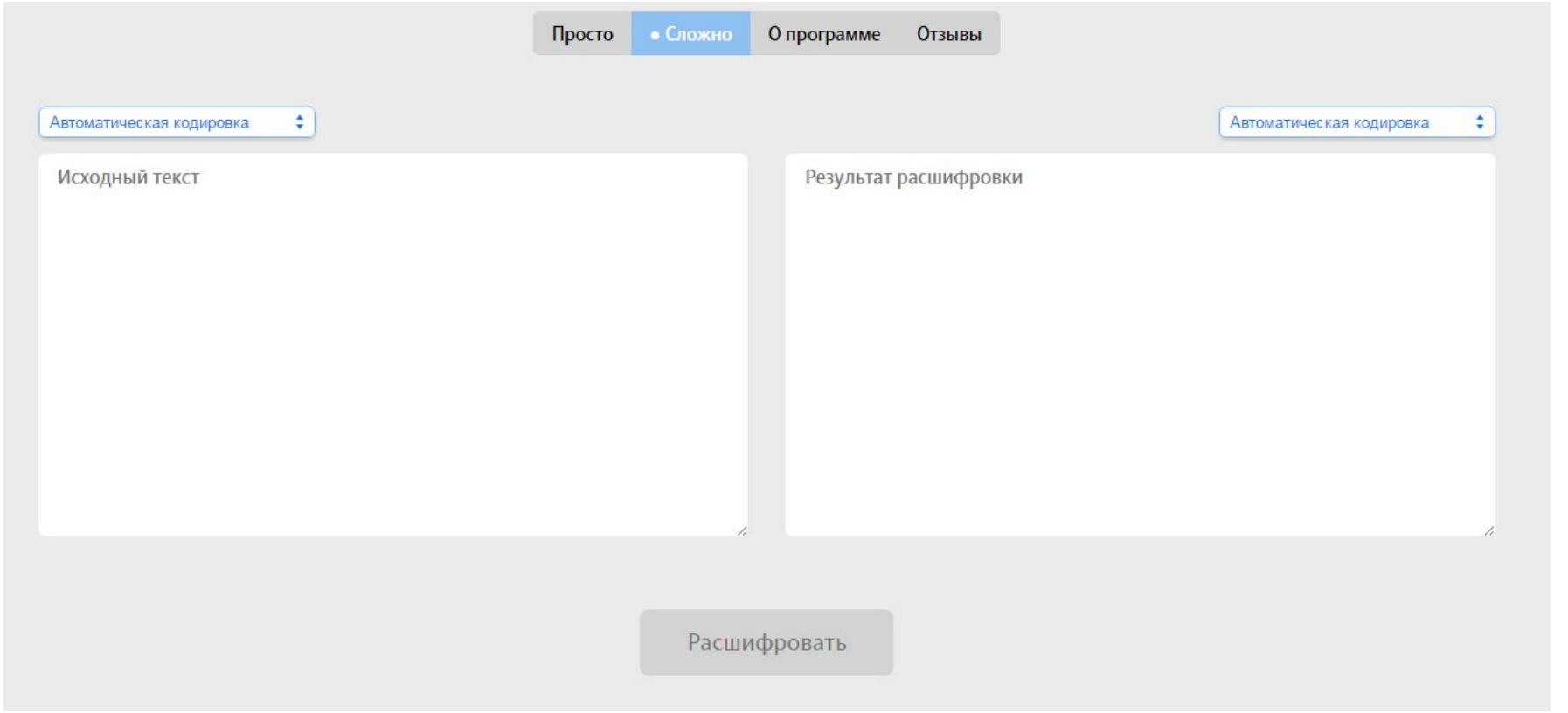
Вот так создаётся шифрованный текст по **шифру скитала**.

Автоматизация криптоанализа

Инструменты

1) Декодер (http://www.artlebedev.ru/tools/decoder/)
2) quipquip (http://www.quipqiup.com/)
3) ViGENER (https://f00l.de/hacking/vigenere.php)
4) xortool (https://github.com/hellman/xortool)
5) CrypTool (https://www.cryptool.org/en/)
6) http://cryptoclub.org/
7) http://planetcalc.ru/733/
8) Скрипты на python
9) PHP
10) **www.dcode.fr**

Декодер


Просто
• Сложно
О программе
Отзывы
Автоматическая кодировка
Автоматическая кодировка
Исходный текст
Результат расшифровки
Расшифровать

Шифр простой замены

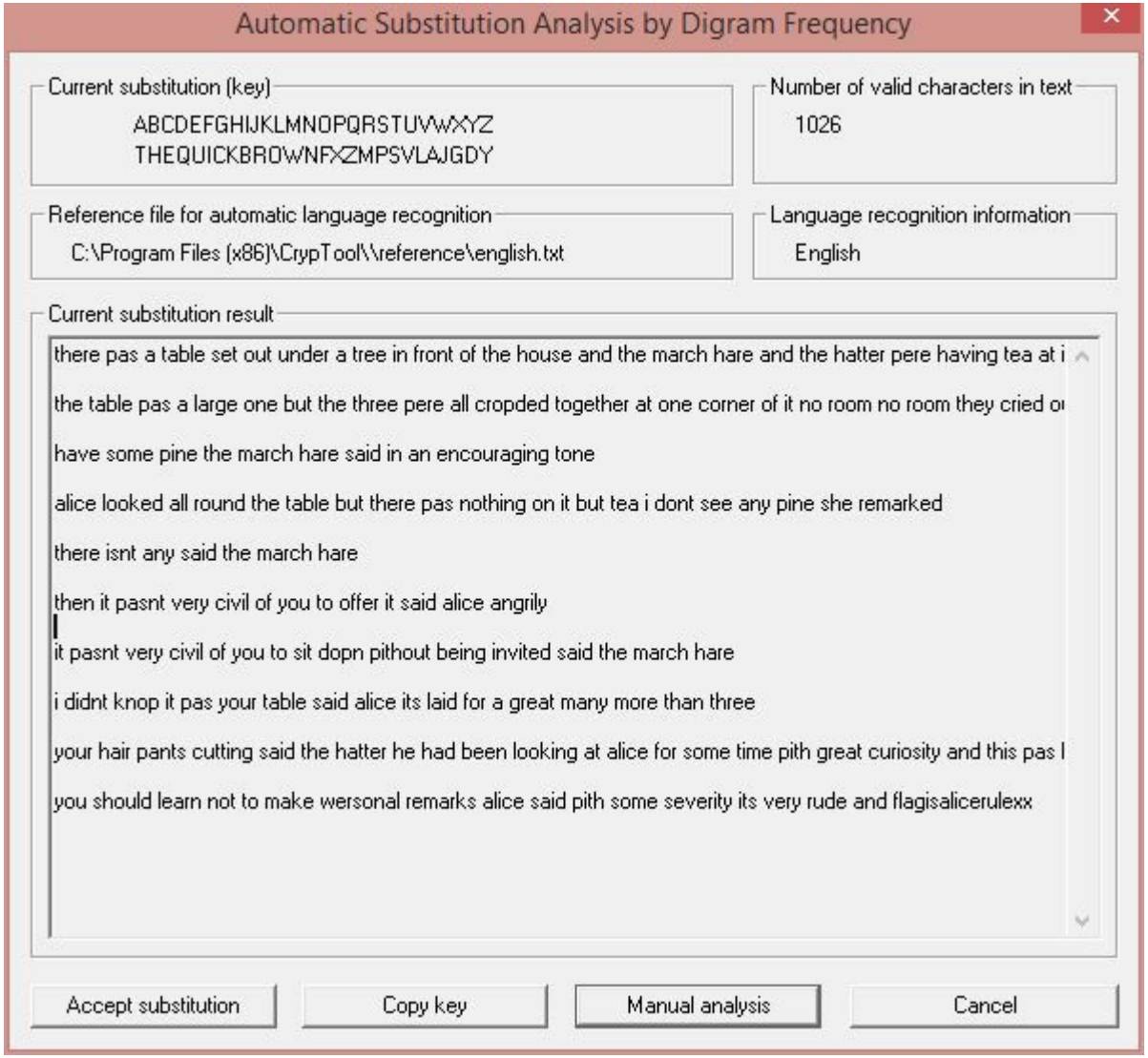
Шифр, относящийся к группе одноалфавитных шифров подстановки. Ключом шифра служит перемешанный произвольным образом алфавит. Например, ключом может быть следующая последовательность букв: XFQABOLYWJGPMRVIHUSDZKNTEC.

При шифровании каждая буква в тексте заменяется по следующему правилу. Первая буква алфавита замещается первой буквой ключа, вторая буква алфавита — второй буквой ключа и так далее. В нашем примере буква A будет заменена на X, буква B на F.

При расшифровке буква сперва ищется в ключе и затем заменяется буквой стоящей в алфавите на той же позиции.

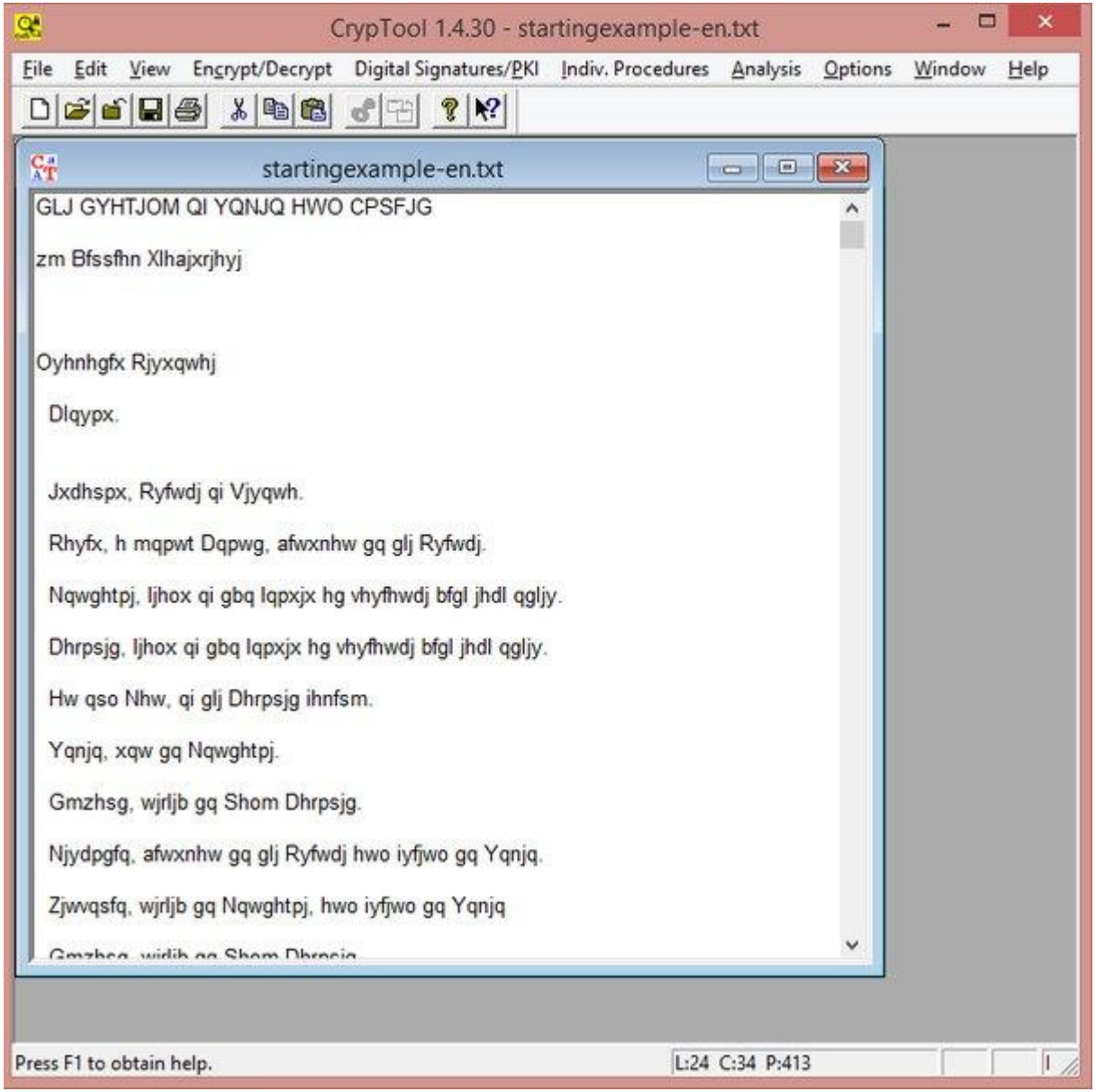
Для вскрытия подобных шифров используется частотный криптоанализ.

Частотный анализ с помощью CrypTool



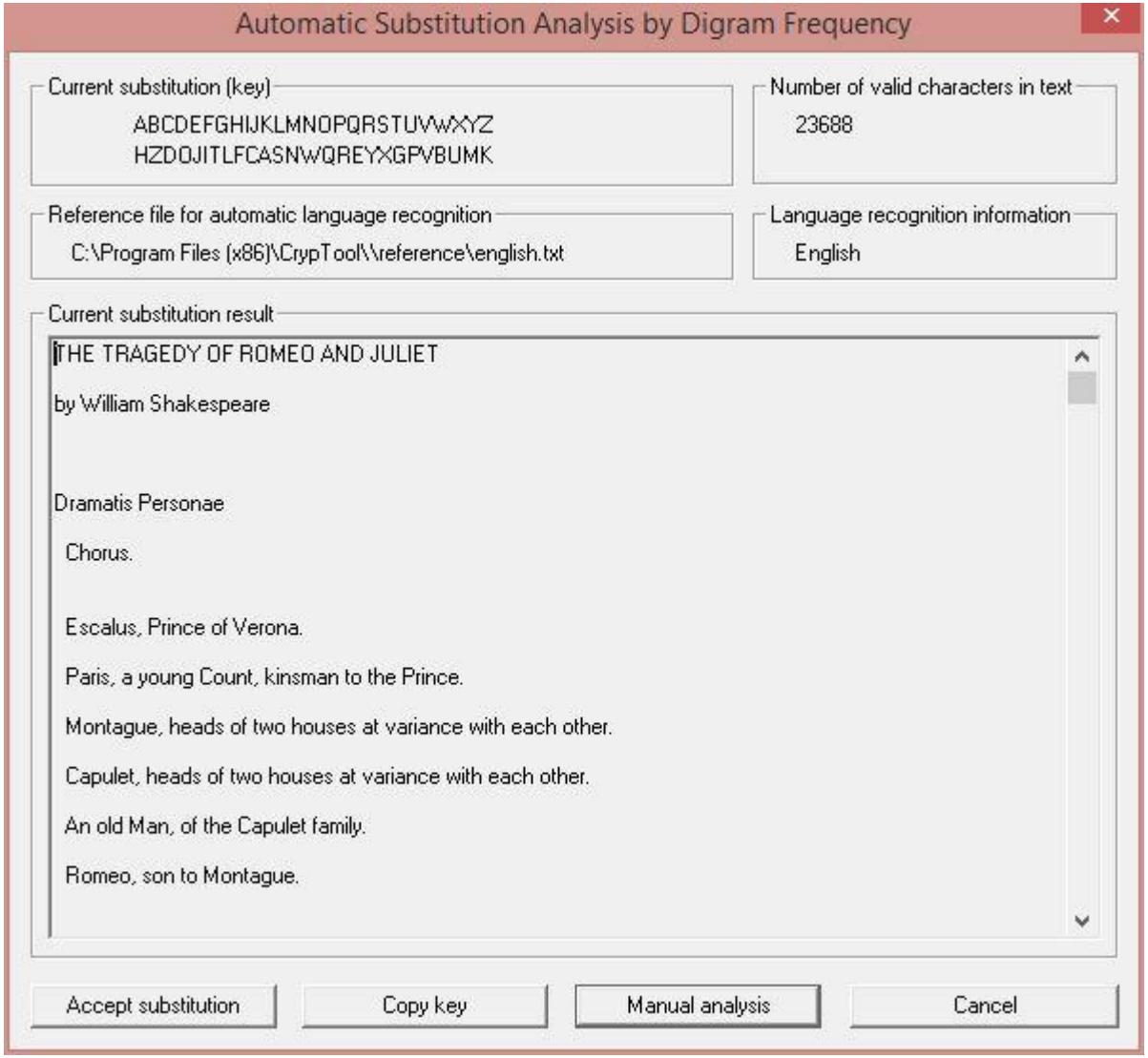
flagisalicerulezz

CrypTool

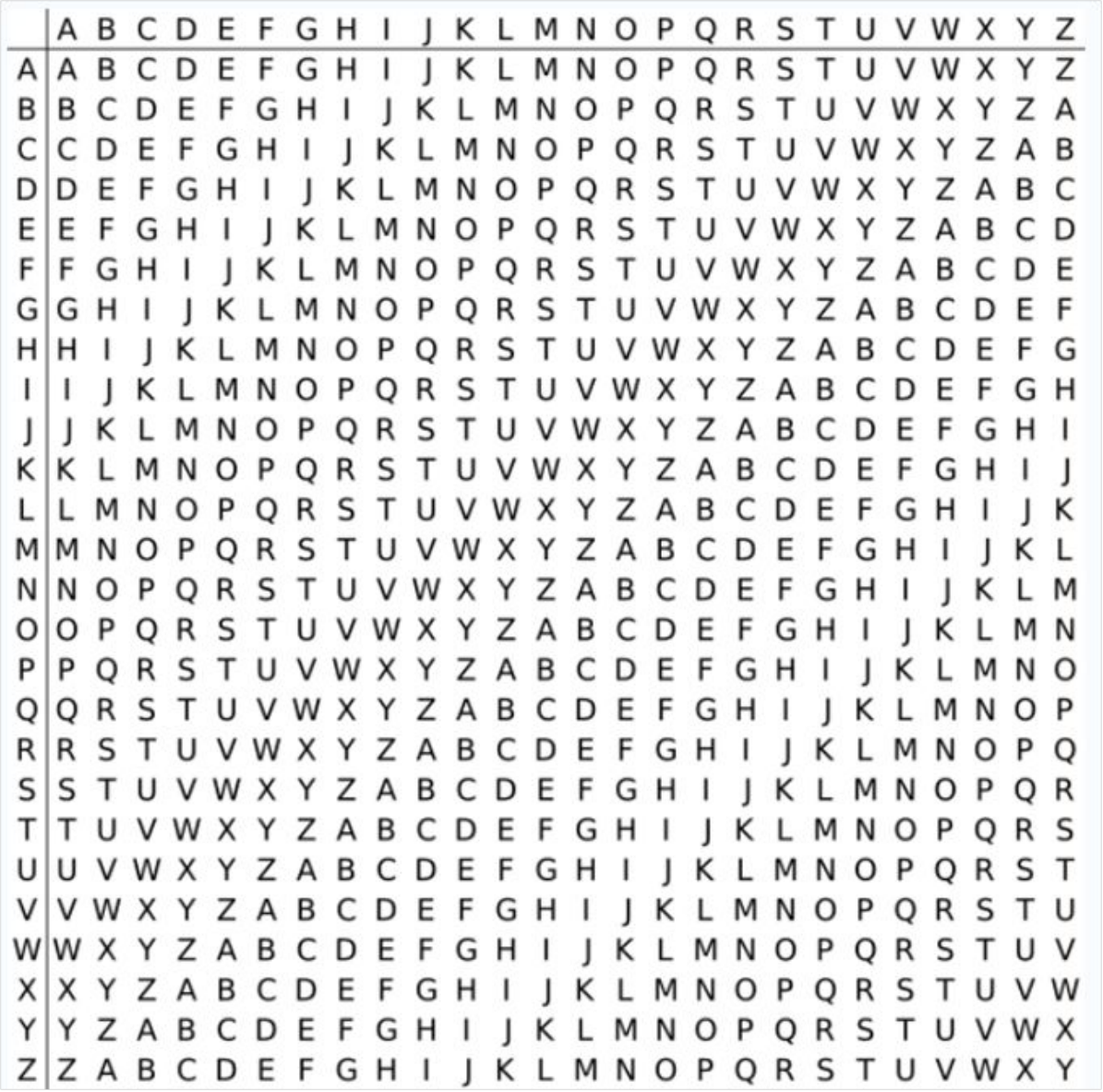

CrypTool 1.4.30 - startingexample-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
GLJ GYHTJOM QI YQNJQ HWO CPSFJG
zm Bfssfhn Xlhajxrjhyj
Oyhnhgfx Rjyxqwhj
Dlqypx.
Jxdhspx, Ryfwdj qi Vjyqwh.
Rhyfx, h mqpwt Dqpwg, afwxnhw gq glj Ryfwdj.
Nqwghtpj, Ijhox qi gbq Iqpxjx hg vhyfhwdj bfgl jhdl qgljy.
Dhrpsjg, Ijhox qi gbq Iqpxjx hg vhyfhwdj bfgl jhdl qgljy.
Hw qso Nhw, qi glj Dhrpsjg ihnfsm.
Yqnjq, xqw gq Nqwghtpj.
Gmzhsg, wjrljb gq Shom Dhrpsjg.
Njydpgfq, afwxnhw gq glj Ryfwdj hwo iyfjwo gq Yqnjq.
Zjwvqsfq, wjrljb gq Nqwghtpj, hwo iyfjwo gq Yqnjq
Press F1 to obtain help.
L:24 C:34 P:413

CrypTool

Analysis -> Symmetric Encryption (classic) -> Ciphertext-Only -> Substitution Дальше программа сама сделает за нас все(Проведет анализ и выдаст исходный текст)



Шифр Виженера



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

Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

Исходный текст:
ATTACKATDAWN

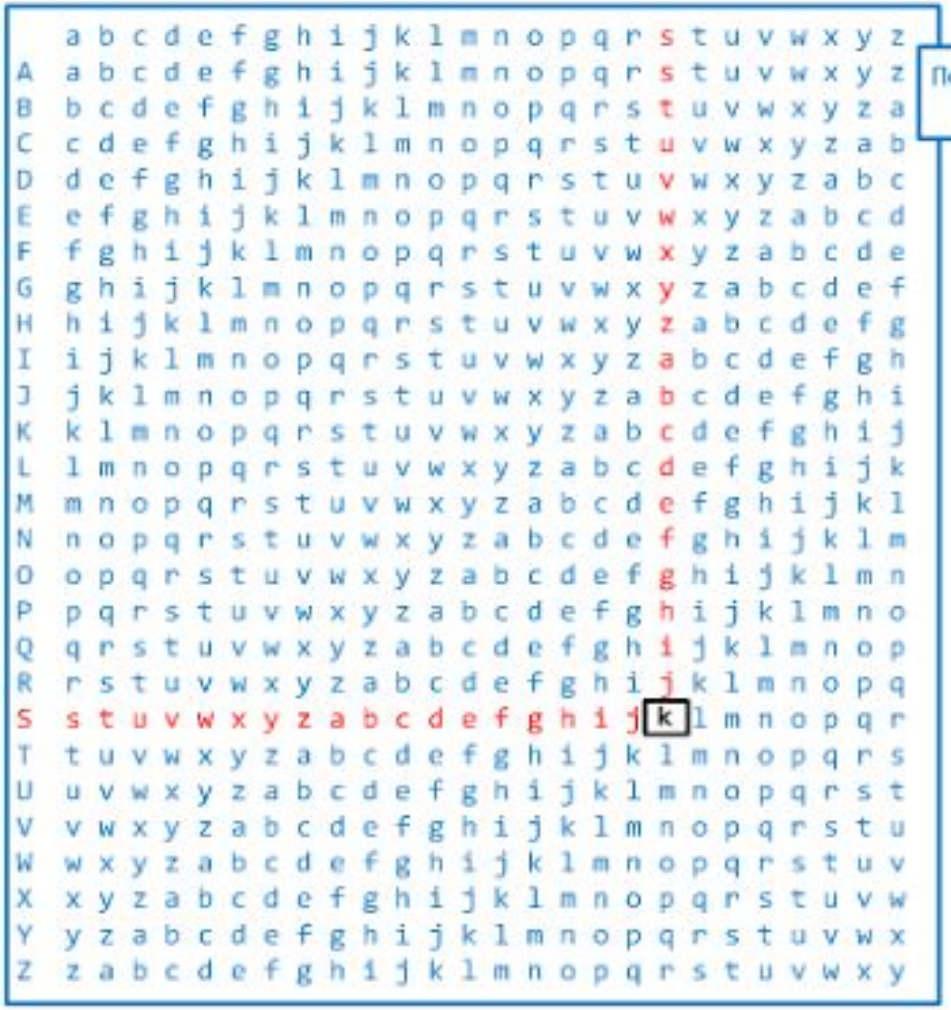
Ключ: **LEMONLEMONLE**

Зашифрованный текст:
LXFOPVEFRNHR

Криптоанализ:

1. Поиск длины ключа.
2. Частотный анализ.

Шифр Виженера



	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
A	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
B	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	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	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

Повторяющийся ключ

```
Securi
System

tySecuri
Security

tyS
And

ecurity
Control

KCUNV UMCUY
TCKGT LVGQH
KZHJL
```

Ключ: SECURITY

Открытый текст сообщения: SYSTEM SECURITY AND CONTROL

Шифротекст сообщения: KCUNV UMCUY TCKGT LVGQH KZHJL

Хеш

Хеш-функция или **функция свёртки** — функция, осуществляющая преобразование массива входных данных произвольной длины в битовую строку установленной длины, выполняемое определённым алгоритмом. Преобразование, производимое хеш-функцией, называется **хешированием**.

«Хорошая» хеш-функция должна удовлетворять двум **свойствам**:

- быстрое вычисление;
- минимальное количество «коллизий».

Применение Хеш-функций

Криптографические хеш-функции

Контрольные суммы

Геометрическое хеширование

Ускорение поиска данных

- **MD 5** c4ca4238a0b923820dcc509a6f75849b (32)
- **SHA-1** 356a192b7913b04c54574d18c28d46e6395428ab **(40)**
- **SHA-256 (64)**
- **SHA-512 (128)**

Практика

http://51.15.83.86:8000