

CTF на Физтехе

Занятие 3

Типы заданий

- Forensics
- Exploitation
- Cryptography
- Web
- Reverse Engineering
- Reconnaissance
- Uucugaga
- ...

Кодировки

ASCII

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	\$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

ANSI Code Pages

Codepage 1251 - Cyrillic Windows

	-0	-1	-2	-3	-4	-5	-6	-7	-8	-9	-A	-B	-C	-D	-E	-F	
0-			0001	0002	0003	0004	0005	0006	0007	0008	0009	000A	000B	000C	000D	000E	000F
1-		0010	0011	0012	0013	0014	0015	0016	0017	0018	0019	001A	001B	001C	001D	001E	001F
2-		!	"	#	\$	%	&	'	()	*	+	,	-	.	/	
3-	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?	
4-	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
5-	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_	
6-	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	
7-	p	q	r	s	t	u	v	w	x	y	z	{		}	~		
8-	Ђ	Ѓ	И	Ј	Љ	Њ	Ћ	Ќ	Ў	Ц	€	‰	Љ	<	Њ	Ѓ	Ћ
9-	ђ	ѓ	и	ј	љ	њ	ћ	ќ	ў	џ	™	љ	>	њ	ћ	џ	џ
A-	Ў	Ў	Ј	Љ	Њ	Ћ	Ќ	Ў	Ц	€	‰	Љ	<	Њ	Ѓ	Ћ	Ћ
B-	°	±	І	і	г	р	џ	·	ё	№	»	ј	Ј	Ѕ	ѕ	ї	
C-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	
D-	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
E-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	
F-	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	

Codepage 1252 - Latin 1 Windows

	-0	-1	-2	-3	-4	-5	-6	-7	-8	-9	-A	-B	-C	-D	-E	-F	
0-			0001	0002	0003	0004	0005	0006	0007	0008	0009	000A	000B	000C	000D	000E	000F
1-		0010	0011	0012	0013	0014	0015	0016	0017	0018	0019	001A	001B	001C	001D	001E	001F
2-		!	"	#	\$	%	&	'	()	*	+	,	-	.	/	
3-	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?	
4-	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
5-	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_	
6-	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	
7-	p	q	r	s	t	u	v	w	x	y	z	{		}	~		
8-	€		,	f	„	…	†	‡	^	‰	Š	<	œ		Ž		
9-		‘	’	“	”	•	—	—	™	š	>	æ		ž	Ÿ		
A-		ı	ç	£	¤	¥	¦	§	¨	©	ª	«	¬	-	®	¯	
B-	°	±	²	³	´	µ	¶	·	¸	¹	º	»	¼	½	¾	¿	
C-	À	Á	Â	Ã	Ä	Å	Æ	Ç	È	É	Ê	Ë	Ì	Í	Î	Ï	
D-	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	×	Ø	Ù	Ú	Û	Ü	Ý	Þ	ß	
E-	à	á	â	ã	ä	å	æ	ç	è	é	ê	ë	ì	í	î	ï	
F-	ð	ñ	ò	ó	ô	õ	ö	÷	ø	ù	ú	û	ü	ý	þ	ÿ	

Unicode

- Каждому символу сопоставлено число от 0 до 0x100000 (code point)

Hello



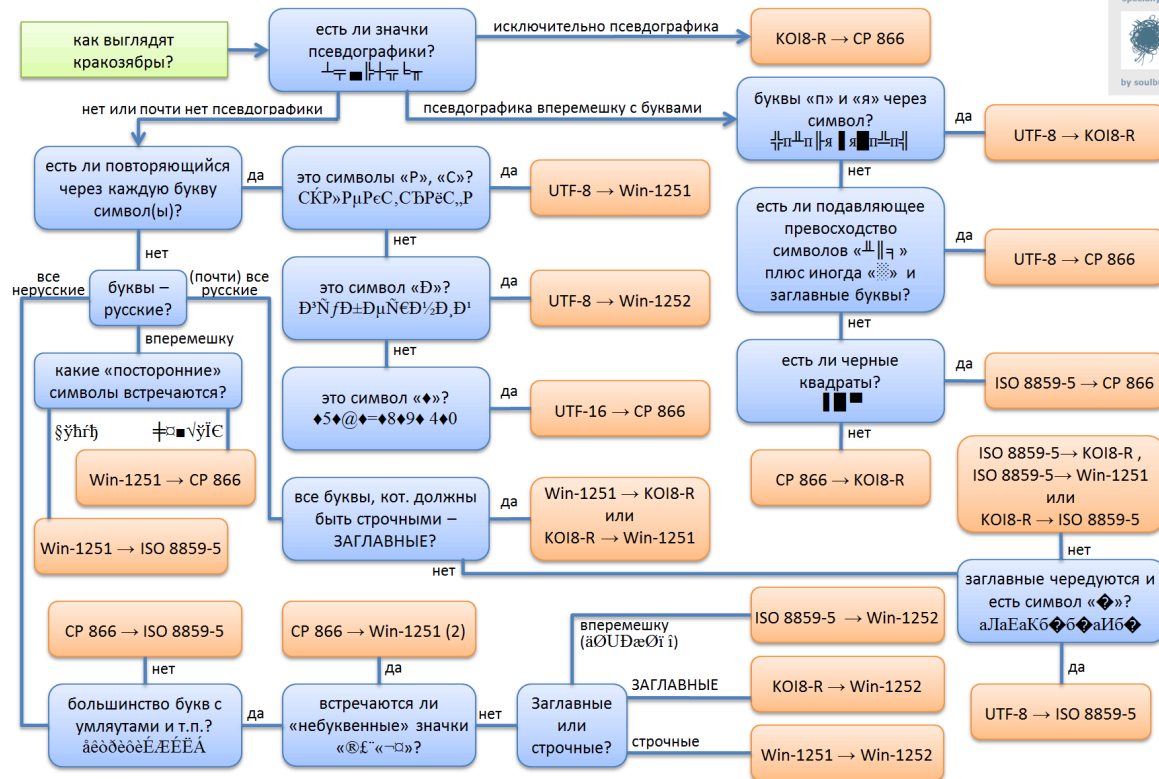
U+0048 U+0065 U+006C U+006C U+006F

UTF-8, UTF-16, UTF-32

- Можно закодировать любой Unicode символ (code point)
- UTF-8: каждый символ 1, 2, 3 или 4 байта
- UTF-16: каждый символ 2 или 4 байта
- UTF-32: каждый символ 4 байта
- **UTF-8 совпадает с ASCII на code point'ax < 128**

Bits of code point	First code point	Last code point	Bytes in sequence	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6
7	U+0000	U+007F	1	0xxxxxxx					
11	U+0080	U+07FF	2	110xxxxx	10xxxxxx				
16	U+0800	U+FFFF	3	1110xxxx	10xxxxxx	10xxxxxx			
21	U+10000	U+1FFFFF	4	11110xxx	10xxxxxx	10xxxxxx	10xxxxxx		
The patterns below are not part of UTF-8, but were part of the first specification.									
26	U+200000	U+3FFFFFFF	5	111110xx	10xxxxxx	10xxxxxx	10xxxxxx	10xxxxxx	
31	U+4000000	U+7FFFFFFF	6	1111110x	10xxxxxx	10xxxxxx	10xxxxxx	10xxxxxx	10xxxxxx

by soulburner



There Ain't No Such Thing As Plain Text

base64

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

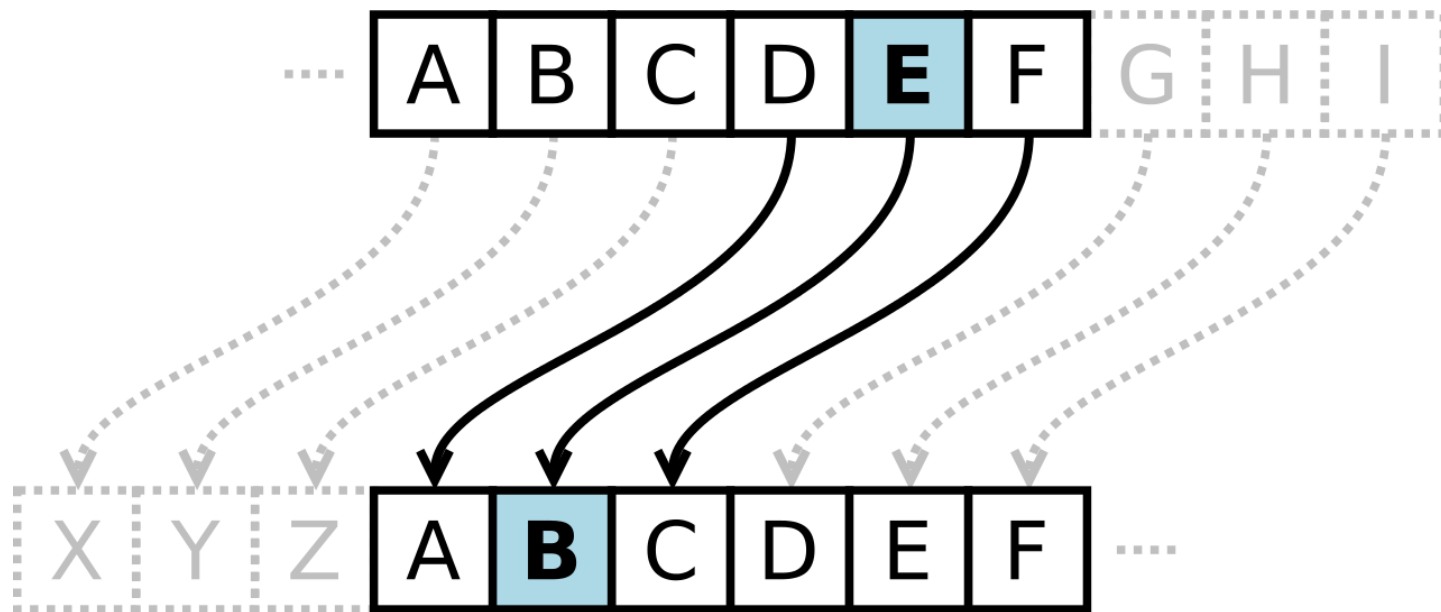
Text content	M				a				n															
ASCII	77 (0x4d)				97 (0x61)				110 (0x6e)															
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Index	19				22				5				46											
Base64-encoded	T				W				F				u											

Winter is coming

V2ludGVyIGlzIGNvbWluZwo=

Классические шифры

Шифр Цезаря

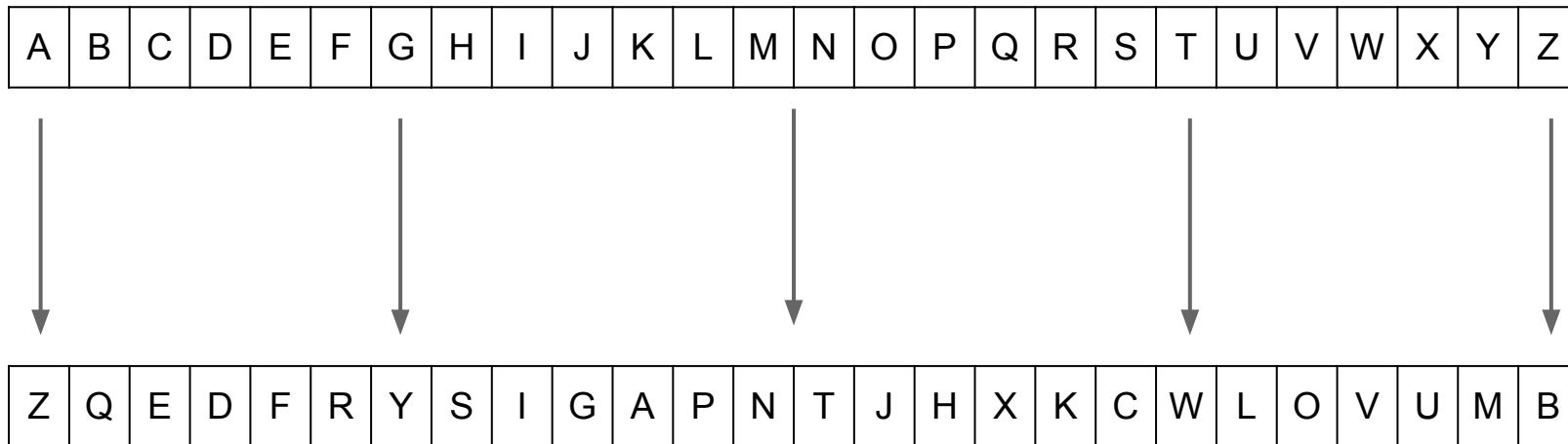


Шифр Цезаря

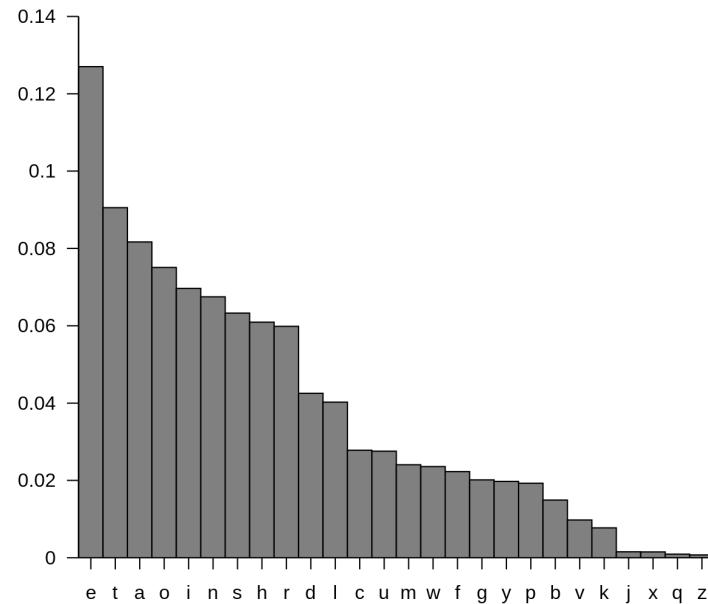
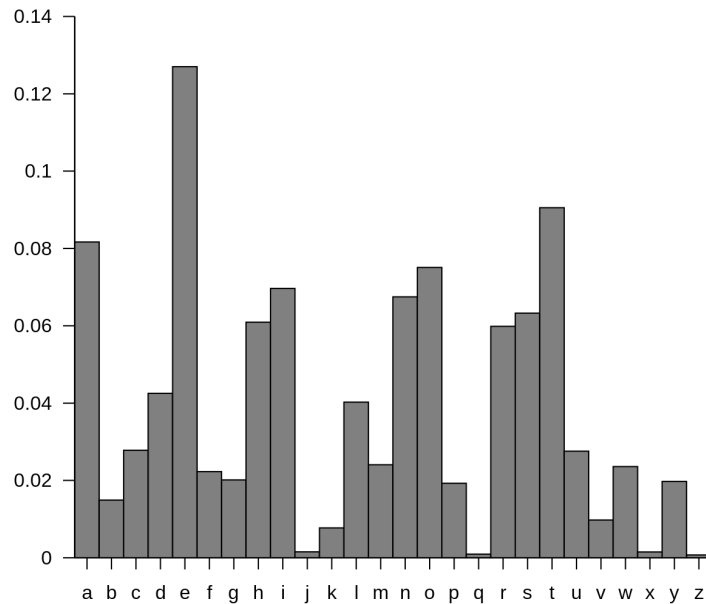
00 JVAGREVPBZVAT
01 KWBHSFWGQCAWBU
02 LXCITGXHRDBXCV
03 MYDJUHYISECYDW
04 NZEKVIZJTFDZEX
05 OAFLOWJAKUGEAFY
06 PBGMXKBLVHFBGZ
07 QCHNYLCMWIGCHA
08 RDIOZMDNXJHDIB
09 SEJPANEOYKIEJC
10 TFKQBOFPZLJFKD
11 UGLRCPGQAMKGLE
12 VHMSDQHRBNLHMF

13 WINTERISCOMING
14 XJOUFSJTDPNJOH
15 YKPVGTKUEQOKPI
16 ZLQWHULVFRPLQJ
17 AMRXIVMWGSQMRK
18 BNSYJWNXHTRNSL
19 COTZKXOYIUSOTM
20 DPUALYPZJVTPUN
21 EQVBMZQAKWUQVO
22 FRWCNARBLXVRWP
23 GSXDOBSCMYWSXQ
24 HTYEPCTDNZXTYR
25 IUZFQDUEOAYUZS

Шифр простой замены



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

Plaintext: WINTERISCOMING

Key: THRONETHRONETH

Ciphertext: PPEHRVBZRCZMGN

Шифр Виженера

В	Л	У	Е	Д	W	Е	С	У	Р	Р	З	У	О	С	Е	Р	Ж	У	О	А	...
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	-----



Длина ключа $L = 6$

- Пусть известна длина ключа L
- Каждый L 'тый символ исходной строки зашифрован с помощью одного и того же символа строки-ключа (шифр Цезаря)
- Используем частотный криптоанализ

Индекс совпадений

- Как определить длину ключа L ?
- Индекс совпадений - вероятность совпадения двух произвольных букв в строке:

$$I = \sum_i \frac{f_i(f_i - 1)}{n(n - 1)}$$

f_i - количество i -ой буквы в строке

n - длина строки

- Для текста на английском индекс совпадений ~ 0.065

L	1	2	3	4	5	6	7	8	9	...
I	0.038	0.043	0.047	0.043	0.038	0.060	0.037	0.042	0.049	...

Делайте то, что нетривиально

- Умеет ли это ваш текстовый редактор?
- Есть ли консольная утилита, которая это делает?
- Можно ли нагуглить веб-инструмент для решения этой задачи?
- Можно ли найти исходный код программы, которая это делает?
- Пишите утилиту сами, только если по всем прочим пунктам - “нет”.

Вопросы?