CTF на Физтехе

Занятие 3

Типы заданий

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

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	Α	97	61	a
2	2	[START OF TEXT]	34	22	II	66	42	В	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	1	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	1	105	69	i
10	Α	[LINE FEED]	42	2A	*	74	4A	J	106	6A	i
11	В	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	С	[FORM FEED]	44	2C	,	76	4C	L	108	6C	1
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	Е	[SHIFT OUT]	46	2E		78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	1	79	4F	0	111	6F	0
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	Р	112	70	р
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	Υ	121	79	V
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	Ĭ.	124	7C	Ĭ
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	1	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

Co	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	8000	0009	GODA	000B	DOOC	0000	000E	000F
1-	0010	0011	0012	0013	0014	0015	0016	0017	0018	0019	001A	001B	001C	001D	001E	001F
2-	0020	6021	11 0022	# 0023	\$ 0024	% 0025	& 0026	0027	(0028)	* 602A	+ 002B	9 002C	- 602D	• 002E	/ 002F
3-	0	1 0031	2	3	4	5	6	7	8	9	003A	9 003B	< 003C	= 003D	> 003E	? 003F
4-	@	A	B 0042	C 0043	D 0044	E 0045	F 0046	G	H 0048	I 0049	J 004A	K 0048	L	M 004D	N 004E	O 004F
5-	P	Q	R 0052	S 0053	T 0064	U 0055	V 0056	W	X 0058	Y 0059	Z	[005B	\ 005C]	↑ 005E	
6-	0060	a	b	C 0063	d	e 0065	f	g	h	i 0069	j	k 0068	1 0060	m 006D	n 006E	0
7-	p	q	r 0072	S 0073	t 0074	u	V 0076	W	X	y	Z	{ 007B	D07C	}	~ 007E	007F
8-	Ъ	Ѓ 0403	, 201A	Γ́ 0453	99 201E	2026	2020	‡ 2021	€ 20AC	% 0	Љ	< 2039	Њ	Ќ 0400	h	Ŭ 040F
9-	ħ 0452	6 2018	9 2019	66 2010	99 201D	2022	2013	2014	0098	TM 2122	Љ 0459	> 203A	Њ 045А	Ќ 045С	ħ 0458	Џ 045F
A-	00A0	Ÿ	ў 045Е	J	¤	Γ 0490	U 00A6	§ 00A7	Ë	© ODA9	€	≪ DDAB	DDAC	- 00AD	® ODAE	Ï 0407
B-	0	± 00B1	I 0406	i 0456	Г 0491	μ	¶	0087	ë	Nº 2116	€	>> 0088	j 0458	S ₀₄₀₅	S 0455	Ï 0457
C-	A 0410	Б	B 0412	Г 0413	Д	E 0415	Ж	3	И 0418	Й	K 041A	Л	M 0410	H 041D	O 041E	П 041F
D-	P ₀₄₂₀	C 0421	T 0422	y	Ф	X 0425	Ц 0426	4	Ш 0428	Щ	Ъ	Ы 0428	Ь 0420	Э	Ю	Я
E-	a 0430	б 0431	B 0432	Г 0433	Д 0434	e 0435	Ж 0436	3	И 0438	й	K 043A	Л 043B	M	H 043D	O 043E	П 043F
F-	p 0440	C 0441	T 0442	y 0443	ф	X 0445	Ц 0446	प 0447	Ш 0448	Щ	Ъ 044А	Ы 044В	b	Э 044D	Ю 044E	Я 044F

Co	depa	ge 1	252 -	Lati	n 1 V	Vind	ows									
	-0	-1	-2	-3	-4	-5	-6	-7	-8	-9	-A	-B	-C	-D	-E	-F
0-		0001	0002	0003	0004	0005	0006	0007	9008	0009	GODA	000B	D00C	000D	000E	000F
1-	0010	0011	0012	0013	0014	0015	0016	0017	0018	0019	001A	001B	001C	001D	001E	001F
2-	0020	0021	11 0022	# 0023	\$ 0024	%	& 0026	0027	(0028)	*	+	9 002C	- 602D	• 002E	/ 002F
3-	0	1	2	3	4	5	6	7	8	9	003A	, 003B	< 003C	= 003D	> 003E	?
4-	@	A	B 0042	C 0043	D 0044	E 0045	F 0046	G	H 0048	I 0049	J	K 0048	L	M 004D	N 004E	O 004F
5-	P 0050	Q	R 0052	S 0053	T	U 0055	V 0056	W 0057	X 0058	Y 0059	Z	0068	\ 005C]	↑ 005E	005F
6-	0060	a	b	C 0063	d	e 0085	f	g	h	i 0069	j	k 0068	l 0060	m 006D	n 006E	0
7-	p	q	r 0072	S	t 0074	u 0075	V	W	X	y	Z	{ 0078	D07C	}	~ 007E	007F
8-	€ 20AC	0081	, 201A	f	99 201E	2026	‡ 2020	2021	0208	% 0	Š 0160	< 2039	Œ 0152	008D	Ž	008F
9-	0090	6 2018	9 2019	66 2010	99 201D	2022	2013	2014	~ 02DC	TM 2122	Š 0161	> 203A	œ 0153	609D	Ž	Ÿ 0178
A-	00A0	00A1	¢ □00A2	£	¤	¥ 00A5	I I 00A6	§ 00A7	•• 00A8	© ODA9	<u>a</u>	≪ 00AB	DOAC	- 00AD	® ODAE	
B-	0	± 00B1	2	3 0083	0084	μ	¶ ∞86	0087	5 00B8	1 0089	<u>0</u>	>> 00BB	1/4 00BC	1/2 00BD	3/4 00BE	¿ OOBF
C-	À	Á 0001	Â	Ã	Ä 00C4	Å	Æ	Ç	È	É	Ê	Ë	Ì	Í	Î	Ï oocf
D-	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	X 0007	Ø	Ù	Ú	Û	Ü	Ý	Þ	ß
E-	à	á	â	ã	ä	å	æ	Ç	è	é	ê OOEA	ë	ì	í	î	i ODEF
F-	ð	ñ 00F1	ò	Ó	ô	Õ	Ö	÷ 00F7	Ø 00F8	ù ^{00F9}	ú ODFA	û OOFB	ü	ý	þ	ÿ

Unicode

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

Hello

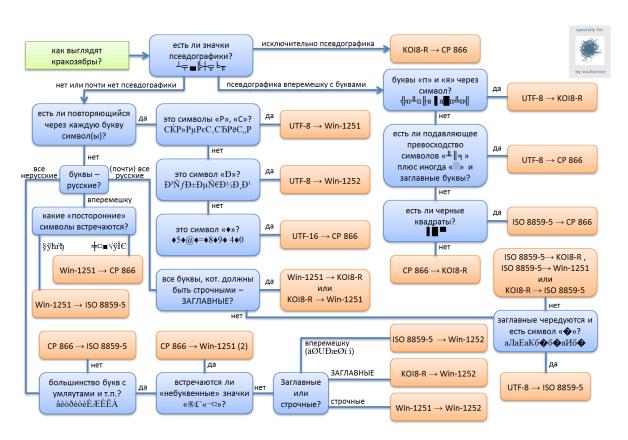
U+0048 U+0065 U+006C U+006C U+006F

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 pattern	s below are n	ot part of UTF-	-8, but were	part of the fir	st specificatio	n.			
26	U+200000	U+3FFFFF	5	111110xx	10xxxxxx	10xxxxxx	10xxxxxx	10xxxxxx	
31	U+4000000	U+7FFFFFF	6	1111110x	10xxxxxx	10xxxxxx	10xxxxxx	10xxxxxx	10xxxxxx

Кракозябры



There Ain't No Such Thing As Plain Text

base64

Value	Char	Value	Char	Value	Char	Value	Char
0	Α	16	Q	32	g	48	W
1	В	17	R	33	h	49	X
2	С	18	S	34	i	50	y
3	D	19	Т	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	Н	23	X	39	n	55	3
8	I	24	Y	40	0	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	С	44	S	60	8
13	N	29	d	45	t	61	9
14	0	30	е	46	u	62	+
15	P	31	f	47	V	63	1

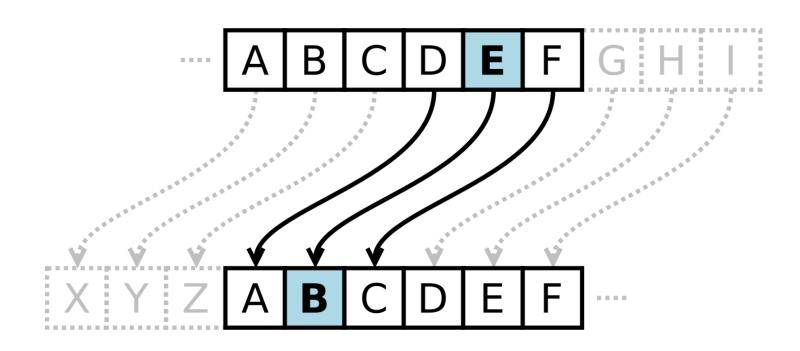
Text content		M						а							n							
ASCII		77 (0x4d))	97 (0x61)								110 (0x6e)							
Bit pattern	0 1 0 0 1 1				0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Index	19				22					5						46						
Base64-encoded		Т					w				F				u			ı				

Winter is coming

V2ludGVylGlzIGNvbWluZwo=

Классические шифры

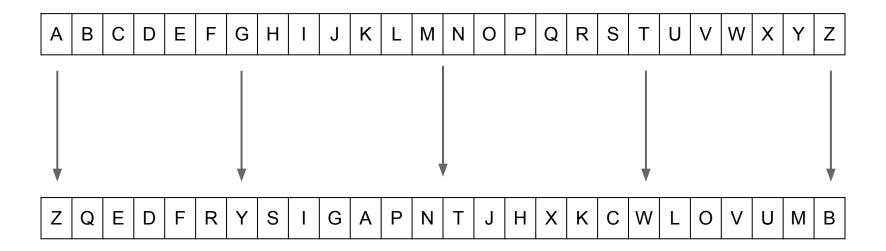
Шифр Цезаря



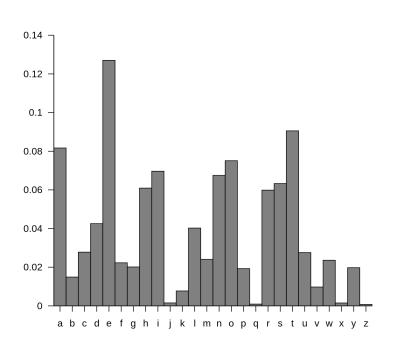
Шифр Цезаря

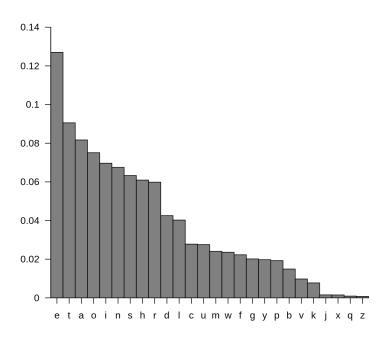
00	JVAGREVFPBZVAT	13	WINTERISCOMING
01	KWBHSFWGQCAWBU	14	XJOUFSJTDPNJOH
02	LXCITGXHRDBXCV	15	YKPVGTKUEQOKPI
03	MYDJUHYISECYDW	16	ZLQWHULVFRPLQJ
04	NZEKVIZJTFDZEX	17	AMRXIVMWGSQMRK
05	OAFLWJAKUGEAFY	18	BNSYJWNXHTRNSL
06	PBGMXKBLVHFBGZ	19	COTZKXOYIUSOTM
07	QCHNYLCMWIGCHA	20	DPUALYPZJVTPUN
08	RDIOZMDNXJHDIB	21	EQVBMZQAKWUQVO
09	SEJPANEOYKIEJC	22	FRWCNARBLXVRWP
10	TFKQBOFPZLJFKD	23	GSXDOBSCMYWSXQ
11	UGLRCPGQAMKGLE	24	HTYEPCTDNZXTYR
12	VHMSDQHRBNLHMF	25	IUZFQDUEOAYUZS

Шифр простой замены



Частотный анализ



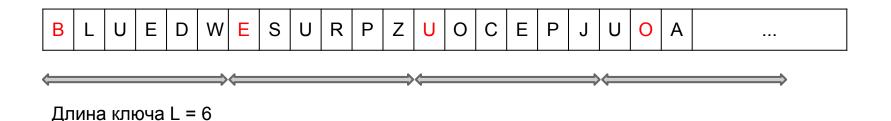


Шифр Виженера

```
AABCDEFGHIJKLMNOPQRSTUVWXYZ
BBCDEFGHIJKLMNOPQRSTUVWXYZA
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
DDEFGHIJKLMNOPQRSTUVWXYZABC
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
 HHIJKLMNOPQRSTUVWXYZABCDEFG
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
LLMNOPQRSTUVWXYZABCDEFGHIJK
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
0 0 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
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 I K L M N O P O 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
XXYZABCDEFGHIJKLMNOPQRSTUVW
YYZABCDEFGHIJKLMNOPQRSTUVWX
ZZABCDEFGHIIKLMNOPORSTUVWXY
```

Plaintext: WINTERISCOMING Key: THRONETHRONETH Ciphertext: PPEHRVBZRCZMGN

Шифр Виженера



- 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:

$$I = \sum_i rac{f_i(f_i-1)}{n(n-1)}$$
 f_i - количество і'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?