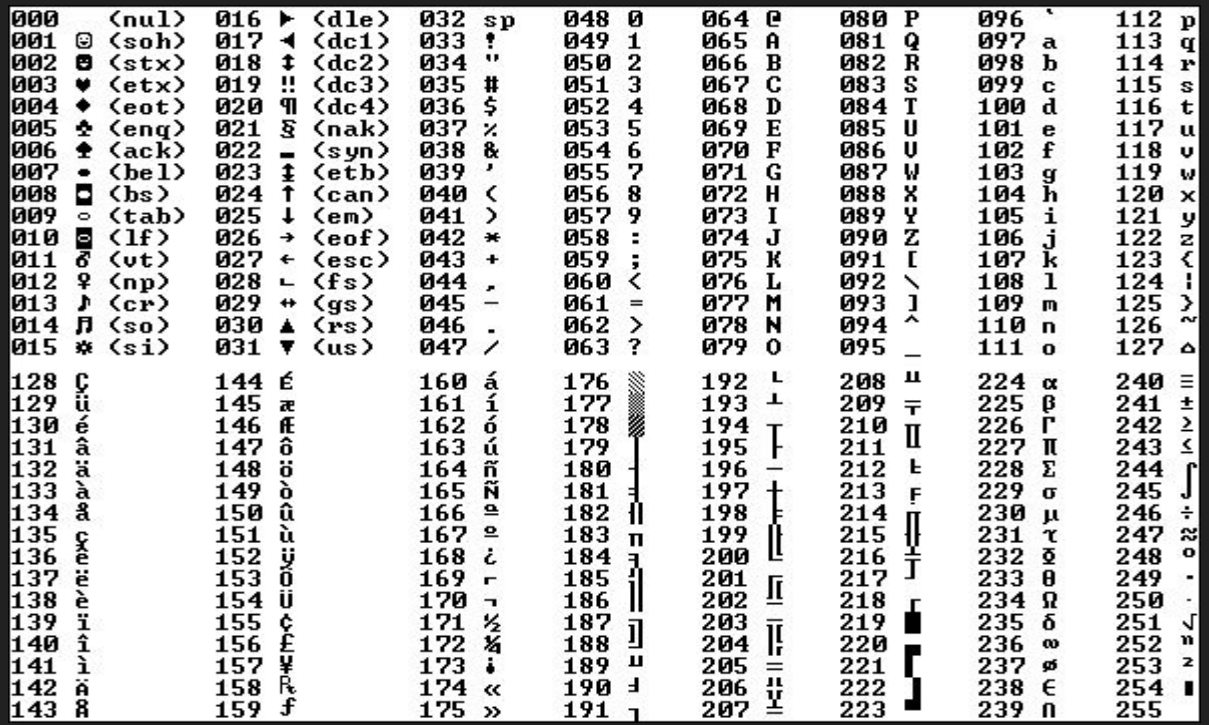
CTF на Физтехе

Занятие 5

ASCII


000 (nul) 016 (dle) 032 sp 048 0 064 @ 080 P 096 ` 112 p
001 (soh) 017 (dc1) 033 ! 049 1 065 A 081 Q 097 a 113 q
002 (stx) 018 (dc2) 034 " 050 2 066 B 082 R 098 b 114 r
003 (etx) 019 (dc3) 035 # 051 3 067 C 083 S 099 c 115 s
004 (eot) 020 (dc4) 036 $ 052 4 068 D 084 T 100 d 116 t
005 (enq) 021 (nak) 037 % 053 5 069 E 085 U 101 e 117 u
006 (ack) 022 (syn) 038 & 054 6 070 F 086 V 102 f 118 v
007 (bel) 023 (etb) 039 ' 055 7 071 G 087 W 103 g 119 w
008 (bs) 024 (can) 040 (056 8 072 H 088 X 104 h 120 x
009 (tab) 025 (em) 041) 057 9 073 I 089 Y 105 i 121 y
010 (lf) 026 (eof) 042 * 058 : 074 J 090 Z 106 j 122 z
011 (vt) 027 (esc) 043 + 059 ; 075 K 091 [107 k 123 {
012 (np) 028 (fs) 044 , 060 < 076 L 092 \ 108 l 124 |
013 (cr) 029 (gs) 045 - 061 = 077 M 093] 109 m 125 }
014 (so) 030 (rs) 046 . 062 > 078 N 094 ^ 110 n 126 ~
015 (si) 031 (us) 047 / 063 ? 079 O 095 _ 111 o 127 ⌂
128 Ç 144 É 160 á 176 ▒ 192 └ 208 ╨ 224 α 240 ≡
129 ü 145 æ 161 í 177 ▒ 193 ┴ 209 ╤ 225 ß 241 ±
130 é 146 Æ 162 ó 178 ▓ 194 ┬ 210 ╥ 226 Γ 242 ≥
131 â 147 ô 163 ú 179 │ 195 ├ 211 ╙ 227 π 243 ≤
132 ä 148 ö 164 ñ 180 ┤ 196 ─ 212 ╘ 228 Σ 244 ⌠
133 à 149 ò 165 Ñ 181 ╡ 197 ┼ 213 ╒ 229 σ 245 ⌡
134 å 150 û 166 ª 182 ╢ 198 ╞ 214 ╓ 230 µ 246 ÷
135 ç 151 ù 167 º 183 ╖ 199 ╟ 215 ╫ 231 τ 247 ≈
136 ê 152 ÿ 168 ¿ 184 ╕ 200 ╚ 216 ╪ 232 Φ 248 °
137 ë 153 Ö 169 ⌐ 185 ╣ 201 ╔ 217 ┘ 233 Θ 249 ∙
138 è 154 Ü 170 ¬ 186 ║ 202 ╩ 218 ┌ 234 Ω 250 ·
139 ï 155 ¢ 171 ½ 187 ╗ 203 ╦ 219 █ 235 δ 251 √
140 î 156 £ 172 ¼ 188 ╝ 204 ╠ 220 ▄ 236 ∞ 252 ⁿ
141 ì 157 ¥ 173 ¡ 189 ╜ 205 ═ 221 ▌ 237 ø 253 ²
142 Ä 158 ₧ 174 « 190 ╛ 206 ╬ 222 ▐ 238 ∈ 254 ■
143 Å 159 ƒ 175 » 191 ┐ 207 ╧ 223 ▀ 239 ∩ 255

Unicode

- UTF-8, UTF-16, UTF-32
- UTF-8:
  - Каждому символу ставиться в соответствие число от 0 до 0x1FFFFF
  - Один символ может быть из 1, 2, 3 или 4 байтов
  - Для символов с кодом < 127 UTF-8 совпадает с ASCII
- UTF-16
  - Один символ может быть из 2 или 4 байтов
- UTF-32
  - Один символ - 4 байта

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	/

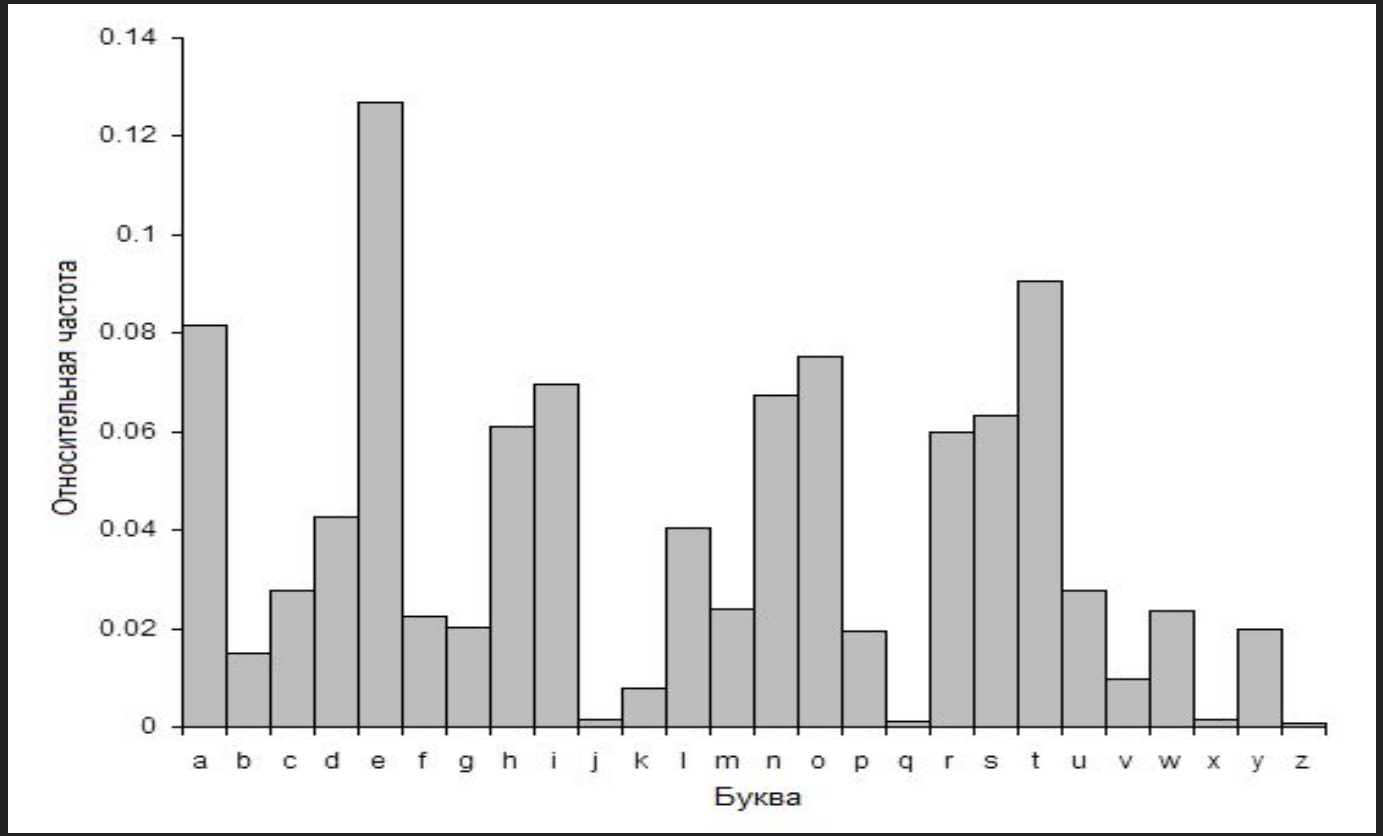
Text content	M							a							n							
ASCII	77							97							110							
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Index	19							22					5				46							
Base64-Encoded	T							W					F				u							

- Man => TWFu
- Hello world => SGVsbG8gd29ybGQ=
- Существует также base32

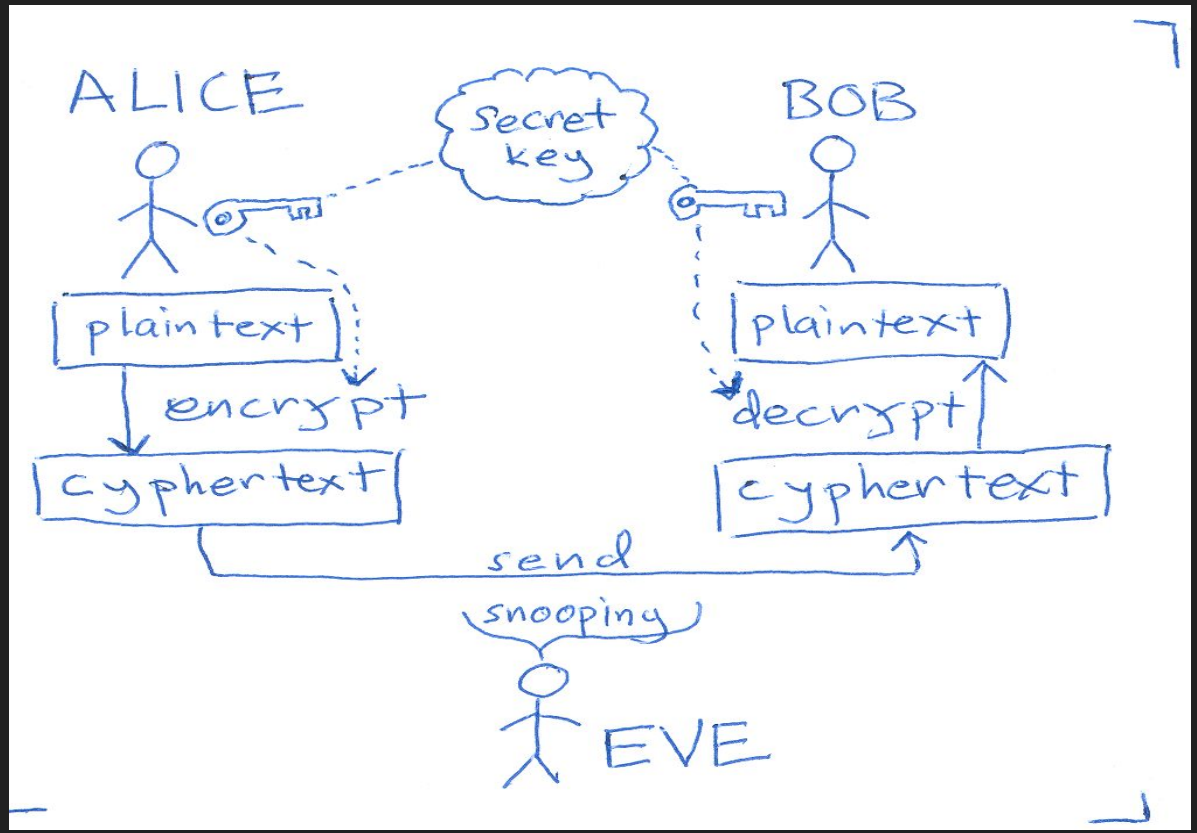
Plaintext

- Как можно различить естественный текст от кракозябр автоматически?
- Визуальный анализ
- Частотный анализ
- Поиск символов, которые не могут быть в естественном тексте (0-31, 127-255)

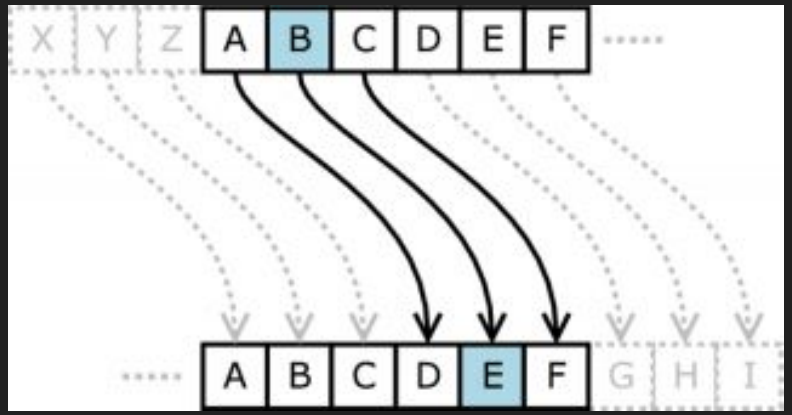
Частотный анализ



Алиса, Боб и Ева



Шифр Цезаря



- Ключ - сдвиг
- Вариантов ключа - 26
- Взламывается “в лоб”

Скитала (спартанский шифр)

Xor

- **a** xor **a** = 0
- **a** xor **b** = **b** xor **a**
- **a** xor **b** = **c:**
  - **a** xor **c** = **b**
  - **b** xor **c** = **a**

x	*y*	*x* XOR *y*
0	0	0
0	1	1
1	0	1
1	1	0

Xor

- Атака - перебор 256 вариантов
- Если длина ключа больше одного байта?
  - Выбираем байты зашифрованные одним и тем же байтом ключа и перебираем независимо
  - Если не знаем длину ключа - перебираем различную длину так, чтобы распределение символов зашифрованных одним и тем же байтом было похоже на распределение естественного текста

Шифр простой замены

- Ключ - перестановка алфавита
- Каждому символу в алфавите сопоставляется другой символ
- Атака - частотный анализ

Шифр Виженера

- Расширение шифра Цезаря
- Ключ - слово

Сообщение	Ключ	Криптограмма
Ш	П	Ж
И	Б	Й
Ф	Е	Щ
Р	П	Я
О	Б	П
В	Е	З
К	П	Щ
А	Б	Б

Шифр Виженера

- Пусть известна длина ключа L
- Каждый L’й символ зашифрован с помощью одного и того же символа ключа(шифр Цезаря)
- Независимо находим каждый символ ключа(частотный анализ)

Подход

- Перед взломом шифра поищите готовое решение
  - Консольная утилита
  - Веб инструмент
- Если таковых нет, тогда пишите свою утилиту

Инструменты

- http://quipqiup.com/ - шифр простой замены
- https://www.cryptool.org/en/
- https://github.com/hellman/xortool
- https://www.artlebedev.ru/tools/decoder/ - кракозябры

Вопросы?