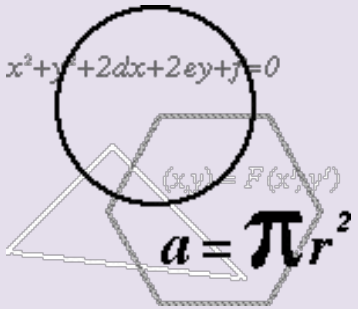
От Цезаря до

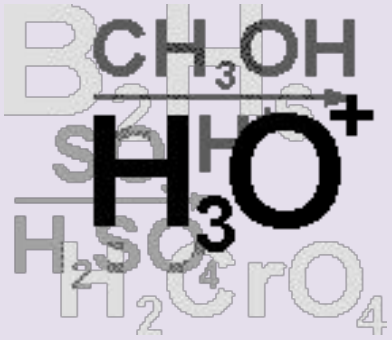
современников

Презентацию выполнила
Николаева Ксения
Ученица 6 «Б» класса

Кодирование информации – это процесс формирования определенного представления информации.

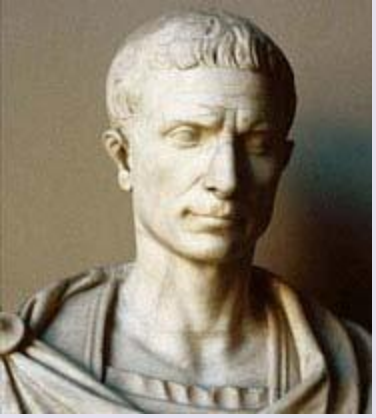
195	11000011
198	11000110
220	11011100
240	11110000
248	11111000
206	11001110
195	11000011
193	11000001



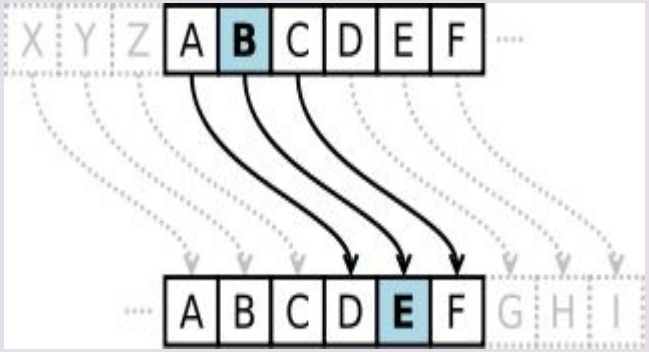


- В более узком смысле под термином «кодирование» часто понимают переход от одной формы представления информации к другой, более удобной для хранения, передачи или обработки.

- С древности люди «засекречивали» информацию, т.е. кодировали.
- Одним из древнейших шифров является шифр Цезаря. Проводя узкую классификацию, шифр можно сравнить с шифром простой замены, потому как используется замена (подстановка) символа другим, находящимся в алфавите на фиксированной позиции от заменяемого.



Шифр Цезаря



- Своё название шифр получил, как вы уже успели догадаться, в честь римского императора Гая Юлия Цезаря (Julius Caesar). Последний использовал шифр для секретной переписки. Однако современный криптоанализ не расценивает шифр Цезаря как шифр приемлемой стойкости. А знали ли вы, что шифр Виженера явился продолжением развития шифра Цезаря?

- Шифр Цезаря подвержен частному анализу, так как является одно-алфавитным шифром подстановки, но это отнюдь не главная «слабость». Так, недостаточное количество ключей - 33 для русского алфавита и 26 для английского – предоставляет возможность проведения атак. Открытый текст вписывается для всех вероятных ключей, а один из вариантов и будет является расшифрованным сообщением.

- Сопоставляя каждому символу порядковый номер, начиная с 9, шифрование и дешифрование выражается формулами:

- Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами:

- $Y=x + k \pmod n$ и $X=y - k \pmod n$, где:
- X — символ открытого текста,
- Y — символ шифрованного текста,
- n — мощность алфавита,
- k — ключ.

- Отметим, что суперпозиция 2х шифрований на ключах K1 и K2 – просто шифрование на ключе K1+K2. В совокупности шифрующие преобразования шифра Цезаря образуют группу Zn.

- К примеру, оригинальный текст: «Съешь же ещё этих мягких французских булок, да выпей чаю».

- Шифрованный текст: «Фэзыя йз зьи ахлш пвёнлш чугрщцкфнлш дцосн, жг еютзм ъгб»

- Используя ключ k = 3, буква С «сдвигается» на три буквы вперед и становится буквой «Ф»; твёрдый знак, перемещённый на три буквы вперед, становится буквой «э», и так далее.

Иоганн Трисемус – шифрующие таблицы

- Многие историки считают Иоганна Трисемуса, аббата из Германии, вторым отцом современной криптологии.
- В 1508 году Трисемус написал “Полиграфию”, первую печатную работу по криптологии. В ней он первым систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке.
- Для получения такого шифра обычно использовались ключевое слово или фраза и таблица, которая для русского языка может иметь размер 5 x 6.
- Ключевое слово вписывалось в таблицу по строкам, а повторяющиеся буквы отбрасывались. Таблица дозаполнялась не вошедшими в нее буквами алфавита по порядку.

- Поскольку ключевое слово легко хранить в памяти, то такой подход упрощал процессы шифрования и дешифрования. Для ключа РЕСПУБЛИКА таблица будет иметь следующий вид:

Р	Е	С	П	У	Б
Л	И	К	А	В	Г
Д	Ж	З	М	Н	О
Т	Ф	Х	Ц	Ч	Ш
Щ	Ь	Ы	Э	Ю	Я

- На основе вышеописанной таблице сообщение ОТПЛЫВАЕМ давало шифровку ШЩАДСНМИЦ.
- Такие табличные шифры называются монограммными, так как шифрование ведется по одной букве.
- Трисемус первым заметил, что можно шифровать по две буквы за раз.
- Такие шифры были названы биграммными. Наиболее известный шифр биграммами называется Playfair. Он применялся Великобританией в Первую мировую войну.

Блез де Виженер – шифр Виженера

- Блезом де Виженером, придворным короля Франции Генриха III, в конце XVI в. был предложен весьма изящный метод шифрования. Иногда этот шифр называют также шифрам с перекрытием текста. Для шифрования используется секретное слово или фраза. Нужно писать это секретное слово над исходным текстом, повторяя его, пока не кончится сообщение. Каждая буква исходного текста заменяется на отстоящую от неё в алфавите на несколько позиций.

- Величина сдвига задаётся буквой ключевого (секретного) слова, стоящей над данной буквой исходного текста. Для буквы А сдвиг вообще отсутствует, буква Б соответствует сдвигу на одну позицию вперёд, буква В — сдвигу на две позиции и так далее. Последняя буква—Я — соответствует сдвигу на 31 позицию, поскольку в русском алфавите 32 буквы. То есть размер сдвига определяется порядковым номером буквы в алфавите, из которого вычтена единица.

Шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому. Но достаточно прост для использования в полевых условиях, особенно если применяются шифровальные диски.

Репродукция шифровального диска Конфедерации

- В примере в качестве ключевого используется слово ХОЛМС. Пусть надо зашифровать сообщение

- ПРИХОДИ НЕМЕДЛЕННО

- Для этого пишется ключевое слово над шифруемой фразой:

ХОЛМСХОЛМСХОЛМСХО
ПРИХОДИНЕМЕДЛЕННО

- Теперь каждую букву сообщения надо сдвинуть вперёд по алфавиту в соответствии с буквой ключевого слова, стоящей над ней. Например, буква Х является двадцать второй буквой алфавита и задаёт сдвиг на двадцать одну позицию вперёд. Вместо буквы П исходного текста получится буква Д зашифрованного сообщения. Вторая буква —Р— исходного сообщения сдвигается в соответствии с буквой О ключевого слова на 14 позиций вперёд и заменяется на букву Ю. И так далее:

- ДЮУБЯЩЦ ШСЭЪТЦСЮВЬ

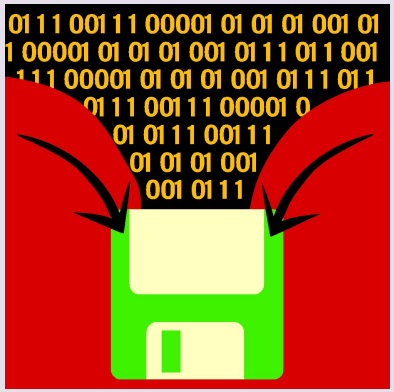
В настоящее время существуют множество способов кодирования информации:

- Штрихкод
- Телеграфное сообщение (код Морзе, код Бодо)
- Морское кодирование (семафорная и флажковая азбука)
- Двоичное кодирование информации

Существует целая наука кодирования информации – криптография и стенография.

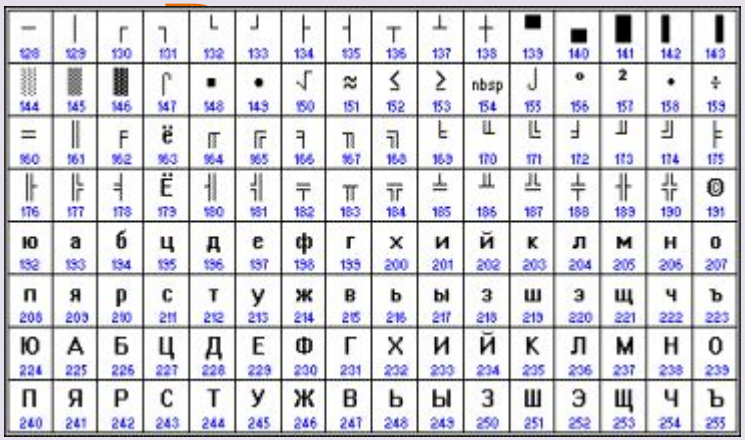
- Компьютер может обрабатывать только информацию, представленную в числовой форме.

- Вся другая информация (звуки, изображения, показания приборов и т. д.) для обработки на компьютере должна быть преобразована в числовую форму.
- Например, чтобы перевести в числовую форму музыкальный звук, можно через небольшие промежутки времени измерять интенсивность звука на определенных частотах, представляя результаты каждого измерения в числовой форме.
- С помощью компьютерных программ можно преобразовывать полученную информацию, например «наложить» друг на друга звуки от разных источников.



Таблицы кодировки русскоязычных символов

КОИ8-



CP1251

CP866

А 128	Б 129	В 130	Г 131	Д 132	Е 133	Ж 134	З 135	И 136	Й 137	К 138	Л 139	М 140	Н 141	О 142	П 143
Р 144	С 145	Т 146	У 147	Ф 148	Х 149	Ц 150	Ч 151	Ш 152	Щ 153	Ъ 154	Ы 155	Ь 156	Э 157	Ю 158	Я 159
а 160	б 161	в 162	г 163	д 164	е 165	ж 166	з 167	и 168	й 169	к 170	л 171	м 172	н 173	о 174	п 175
▒ 176	▓ 177	▓ 178	│ 179	┤ 180	╡ 181	╢ 182	╖ 183	╕ 184	╣ 185	║ 186	╗ 187	╝ 188	╜ 189	╛ 190	┐ 191
└ 192	┴ 193	┬ 194	├ 195	─ 196	┼ 197	╞ 198	╟ 199	╚ 200	╔ 201	╩ 202	╦ 203	╠ 204	═ 205	╬ 206	╧ 207
╨ 208	╤ 209	╥ 210	╙ 211	╘ 212	╒ 213	╓ 214	╫ 215	╪ 216	┘ 217	┌ 218	▒ 219	▒ 220	▒ 221	▒ 222	▒ 223
р 224	с 225	т 226	у 227	ф 228	х 229	ц 230	ч 231	ш 232	щ 233	ъ 234	ы 235	ь 236	э 237	ю 238	я 239
Ё 240	ё 241	Є 242	є 243	Ї 244	ї 245	Ў 246	ў 247	° 248	∙ 249	· 250	√ 251	№ 252	¤ 253	■ 254	nbsp 255

Литература:

1. Википедия

2. Сафаров Т.А. Технология кодирования. Уфа: Башкортостан, 2000

3. Арманд В.А. Железнов В.В. коды в системах обработки информации (интернет-издание)

4. Белов Г.В. Штриховое кодирование: технологии XXI века М.: Металлургия, 1998