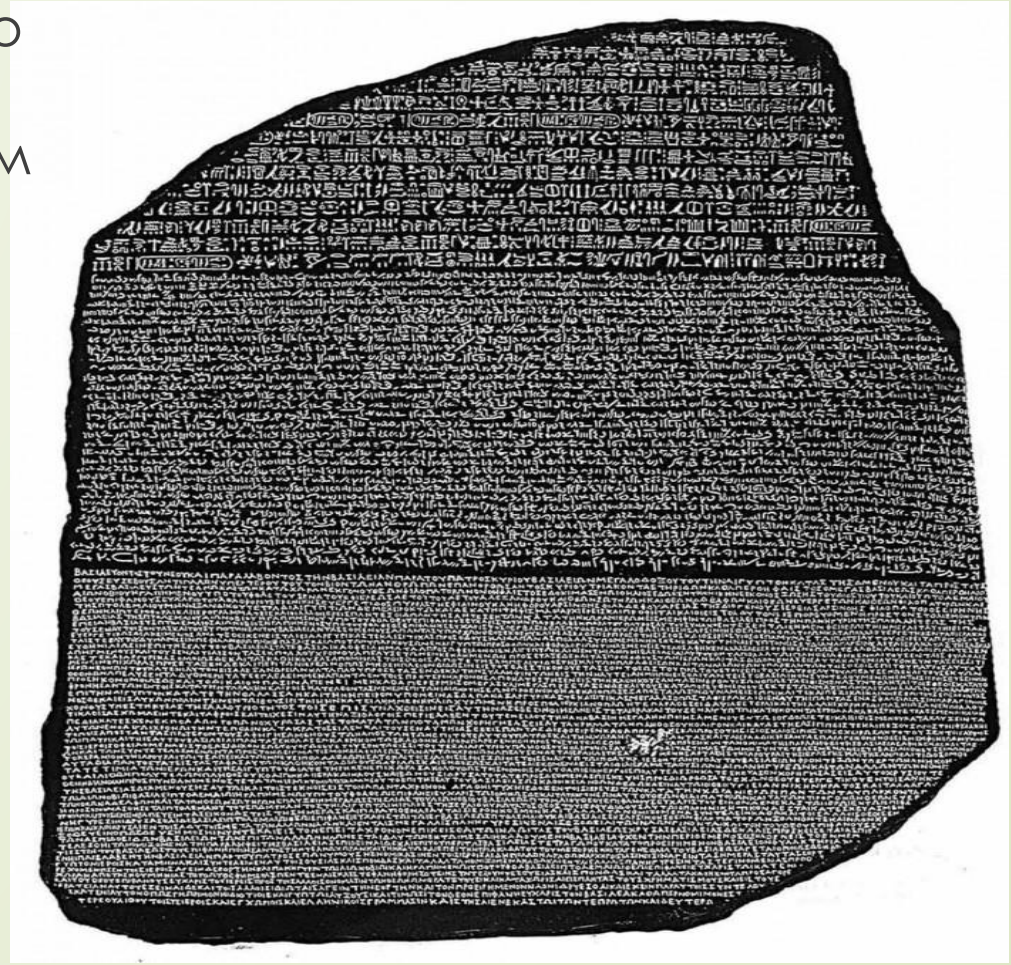
КРИПТОГРАФИЯ

Орындаған:Жақсылық Айгерым

ВОЗНИКНОВЕНИЕ КРИПТОГРАФИИ

История криптографии насчитывает несколько тысячелетий. Первые письменные источники относятся к 1900-м годам до н. э. Именно этим периодом датируются найденные в Египте свитки, в которых использованы видоизмененные иероглифы, по-видимому применявшиеся для тайного обмена сведениями.



Зачем нужна криптография

Как передать нужную информацию нужному адресату в тайне от других?

1. *Создать абсолютно надежный, недоступный для других канал связи между абонентами.*
2. *Использовать общедоступный канал связи, но скрыть сам факт передачи информации.*
3. *Использовать общедоступный канал связи, но передавать по нему информацию в преобразованном виде, чтобы восстановить ее мог только адресат.*

Зачем нужна криптография

До сих пор не разгаданные шифры **Манускрипт Войнича**

Это 240-страничная книга, написанная на абсолютно неизвестном языке с цветными рисунками и странными диаграммами, изображениями невероятных событий и растений, которые не похожи ни на один известный вид.

До сих пор не разгаданные шифры **Криптос**

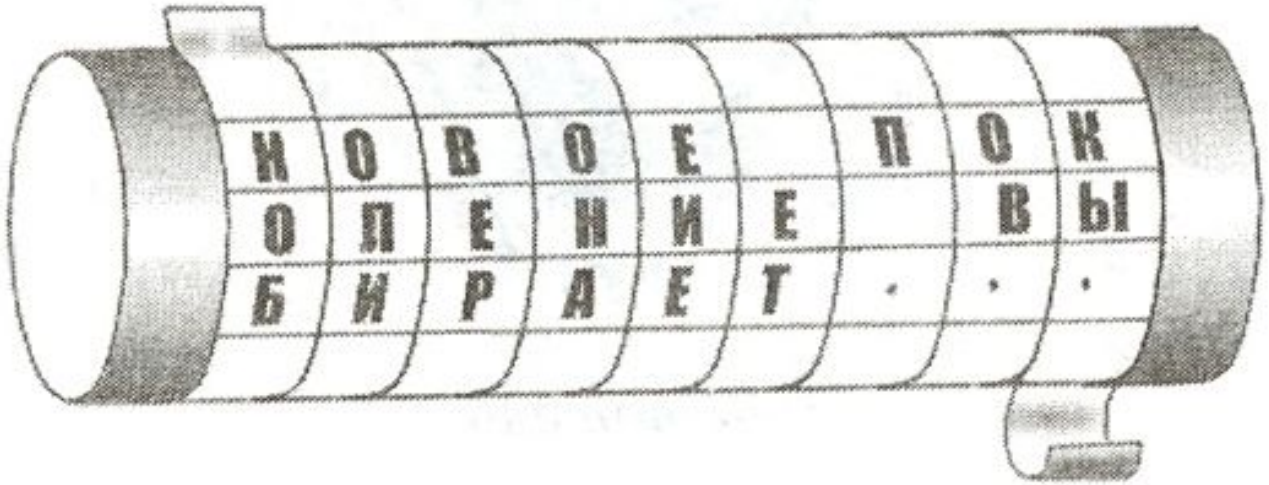
Скульптура, созданная художником Джимом Санборном, которая расположена перед штаб-квартирой Центрального разведывательного управления в Лэнгли, Вирджиния. Скульптура содержит в себе четыре шифровки, вскрыть код четвёртой не удаётся до сих пор. В 2010 году было раскрыто, что символы 64-69 NYPVTT в четвёртой части означают слово БЕРЛИН

До сих пор не разгаданные шифры **Шифр Бэйла**

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975,
14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485,
604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225, 401, 370,
11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500,
538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283,
118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21,
24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131,
160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62,
116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568,
614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4,
30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461,
44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 71, 216,
728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 824, 5,
81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86,
36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985,
233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62,
194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895,
10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62,
31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31,
86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 122, 216,
548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56,
216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617,
84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543, 897, 624, 18,
212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88,
612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132,
40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324, 403, 912, 227, 936,
447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323, 428, 601, 203, 124, 95, 216,
814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84,
221, 736, 820, 214, 11, 60, 760.

Шифр Бэйла — три зашифрованных сообщения, которые, как предполагается, содержат сведения о местонахождении клада из двух фургонов золота, серебра и драгоценных камней, зарытого в 1820-х годах под Линчбергом, что в округе Бедфорд, штат Виргиния, партией золотоискателей под предводительством Томаса Джефферсона Бейла. Цена не найденного доныне клада в пересчете на современные деньги должна составлять около 30 млн долларов. Загадка криптограмм не раскрыта до сих пор, в частности, спорным остается вопрос о реальном существовании клада. Одно из сообщений расшифровано - в нем описан сам клад и даны общие указания на его местоположение. В оставшихся нераскрытыми письменах, возможно, содержатся точное место закладки и список владельцев клада.

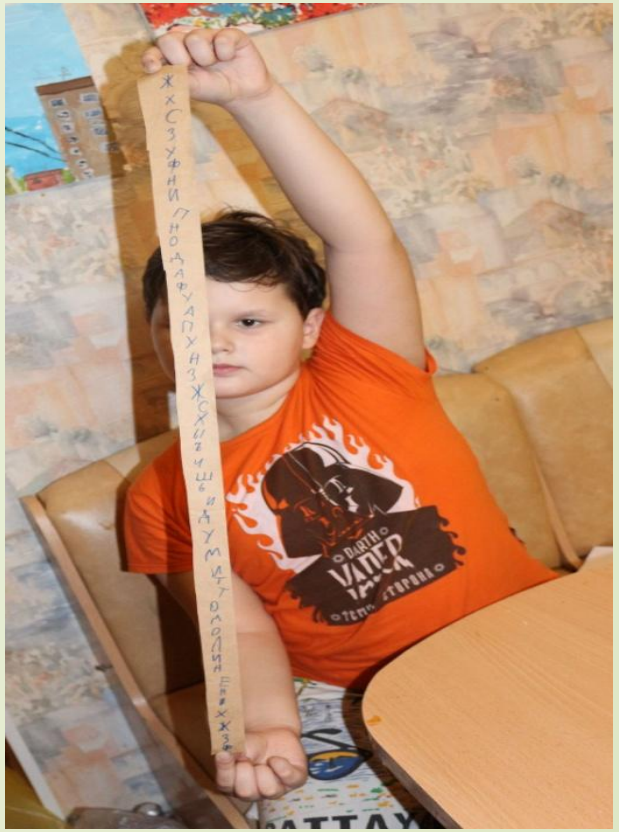
Шифр Сцитала



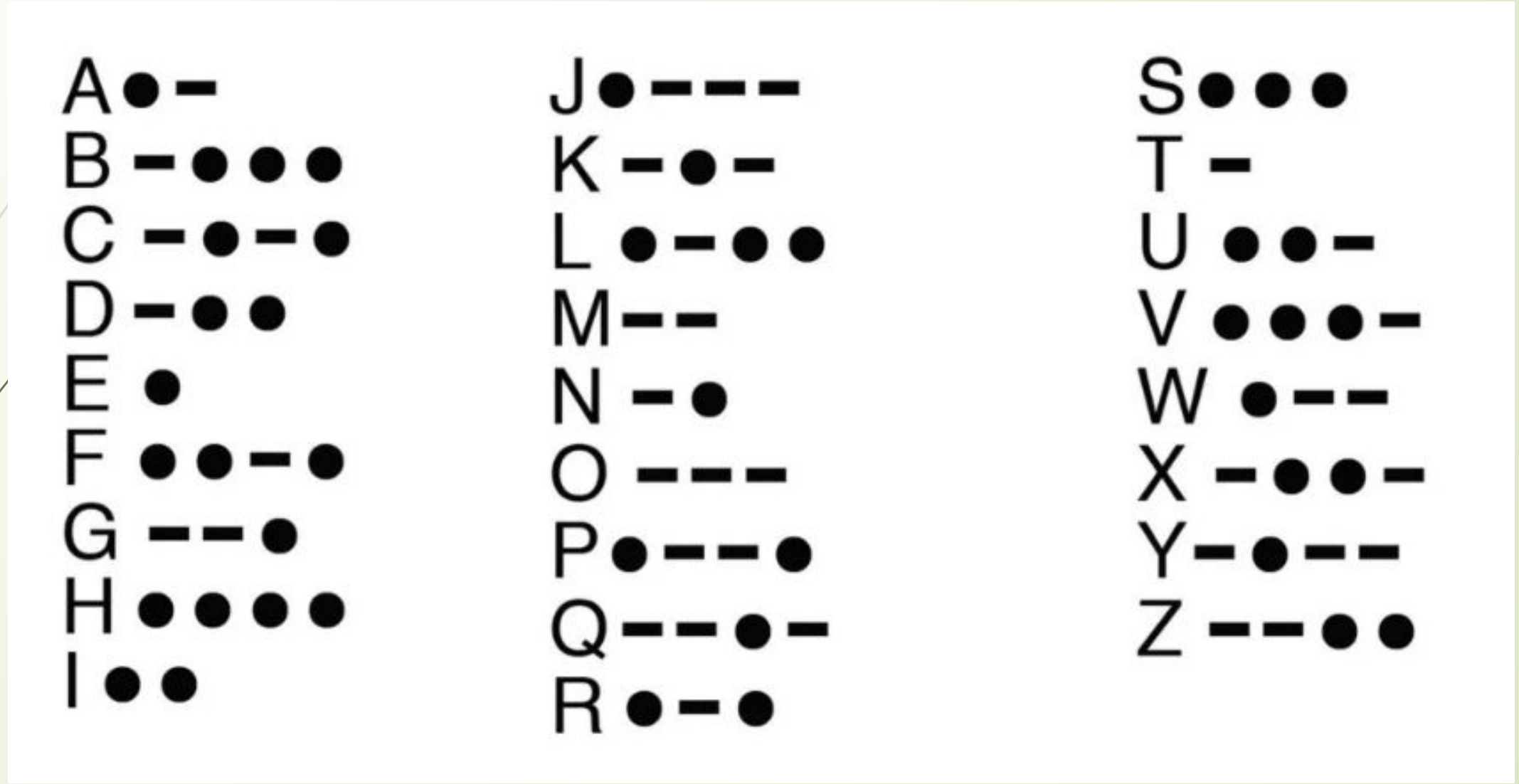
Ключом данного шифра являлся диаметр палки (сциталы).

Шифр Скитала - мой вариант

В качестве основы мы с мамой взяли рулон бумаги, намотали на него полоску бумаги. Я написал сообщение «Спасите». А остальные буквы написал в произвольном порядке



Азбука Морзе



Шифры замены

Шифрами замены называются такие шифры, преобразования в которых приводят к замене каждого символа открытого сообщения на другие символы - *шифробозначения*, причем порядок следования шифробозначений совпадает с порядком следования соответствующих им символов открытого сообщения.

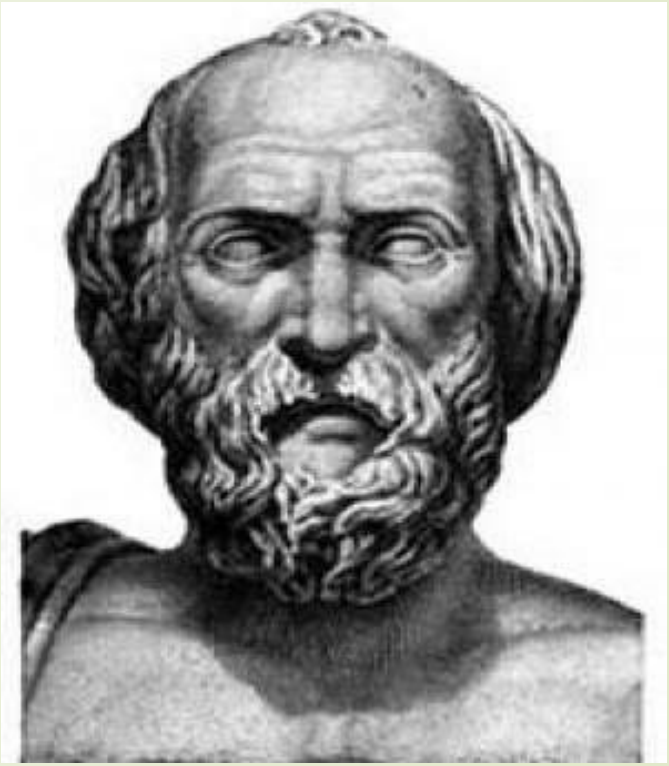
Шифры Темура и Атбаш

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п
я	ю	э	ы	ь	щ	ш	ч	ц	х	ф	у	т	с	р

В 600 - 500 годы до н. э. на Ближнем Востоке древними евреями был разработан один из первых систематических шифров; этот метод называется темура — «обмен». Буквы еврейского алфавита делились на две части, причем одна помещалась над другой; затем верхние буквы заменялись на нижние или наоборот. При этом можно было составлять всевозможные комбинации в зависимости от места разделения алфавита и направления перемещаемых букв. Самый простой способ заключался в разделении алфавита посередине так, чтобы первые две буквы, А (Алеф) и Б (Бет), совпадали с двумя последними, Т (Тае) и Ш (Шин). Эти буквы и дали название методу шифровки — «Атбаш». В России система шифрования «Атбаш» получила широкое распространение в 16-18 веках и название «тарабарская грамота».

Шифр Полибия

Греческий писатель Полибий использовал систему сигнализации, которая была широко принята как метод шифрования. Он записывал буквы алфавита в квадратную таблицу и заменял их парой чисел, которые указывали соответственно на номер строки и номер столбца, на пересечении которых находилась зашифровываемая буква.
При передачи сообщений между сторожевыми вышками тех времен использовались факелы. Так, чтобы передать букву В необходимо было взять 4 факела в правую руку и 3 – в левую. Полибий использовал это для шифрования сообщений и стал записывать каждую букву парой координат.



Шифр Полибия

В нашей стране принцип использования таблицы Полибия нашел широкое применение в 19 веке в среде революционеров, находящихся в тюремном заключении. Революционерами использовались различные наборы алфавитов (то есть опускалось различное число редко встречающихся букв русского языка) и различные размеры таблиц для перестукивания друг с другом через стены камер. Такие системы получили название «тюремных шифров».

	1	2	3	4	5
1	К	Р	Б	Ю	Ы
2	Ф	Т	А	Щ	О
3	Д	Н	Я	И	Е
4	С	Ь	В	М	Ш
5	Э	Г	Л	Ц	П
6	Ж	У	Х	З	Ч

Квадрат Полибия

Усложненные варианты :

Произвольный порядок букв в квадрате.

Ключ-пароль вписывается без повтора букв в квадрат, в оставшиеся клетки – в алфавитном порядке буквы, отсутствующие в пароле.

Шифр Полибия → «тюремный шифр»

Квадрат Полибия

	1	2	3	4	5
1	К	Р	Б	Ю	Ы
2	Ф	Т	А	Щ	О
3	Д	Н	Я	И	Е
4	С	Ь	В	М	Ш
5	Э	Г	Л	Ц	П
6	Ж	У	Х	З	Ч

Например, при шифровании слова «Греция» получим следующую криптограмму:

52 12 35 54 34 33

Квадрат Полибия

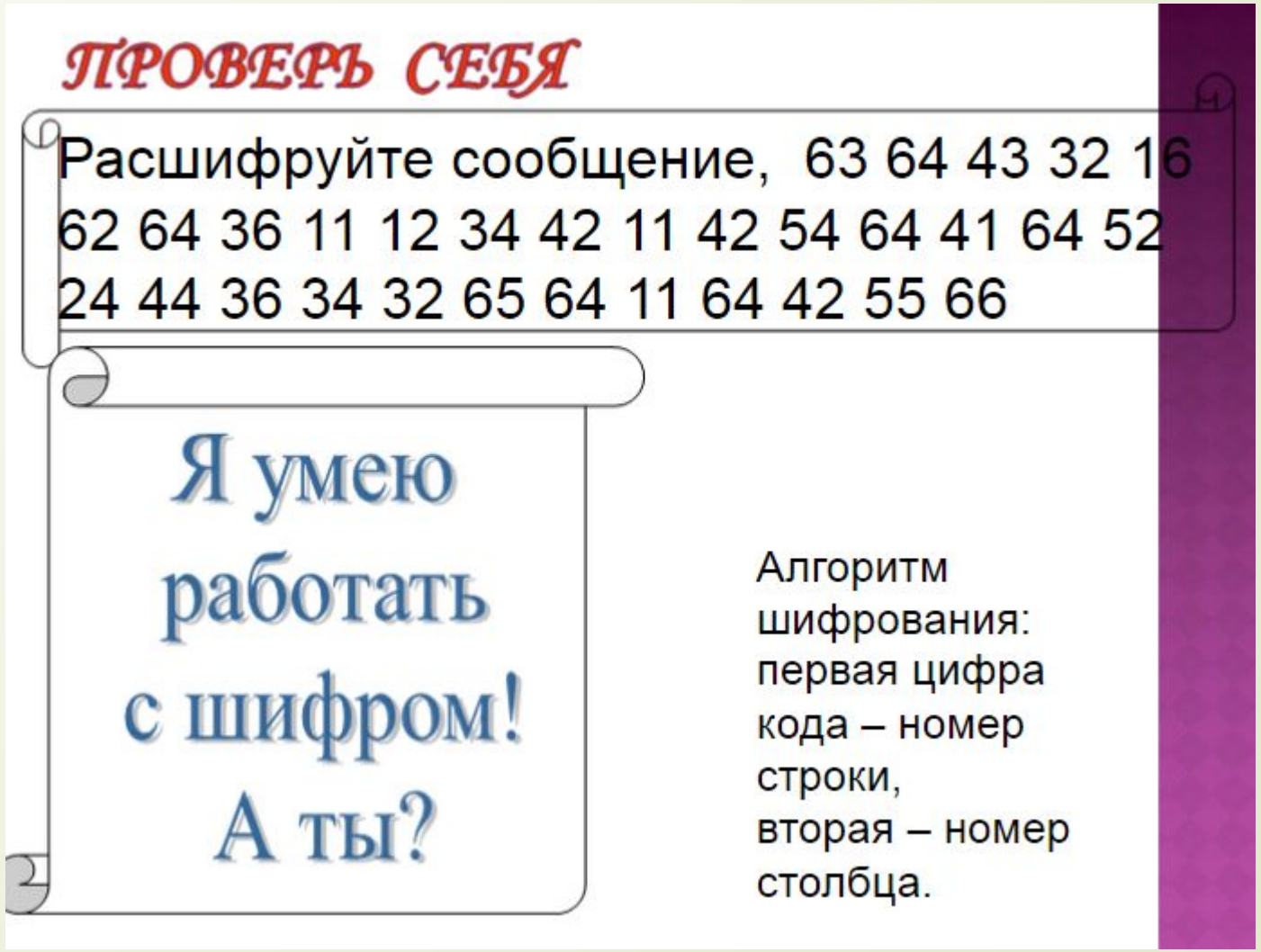
ПРОВЕРЬ СЕБЯ

Расшифруйте сообщение, 63 64 43 32 16
62 64 36 11 12 34 42 11 42 54 64 41 64 52
24 44 36 34 32 65 64 11 64 42 55 66

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ь	Ы	Ъ
6	Э	Ю	Я		!	?

Алгоритм шифрования: первая цифра кода – номер строки, вторая – номер столбца.

Квадрат Полибия



Шифр Цезаря

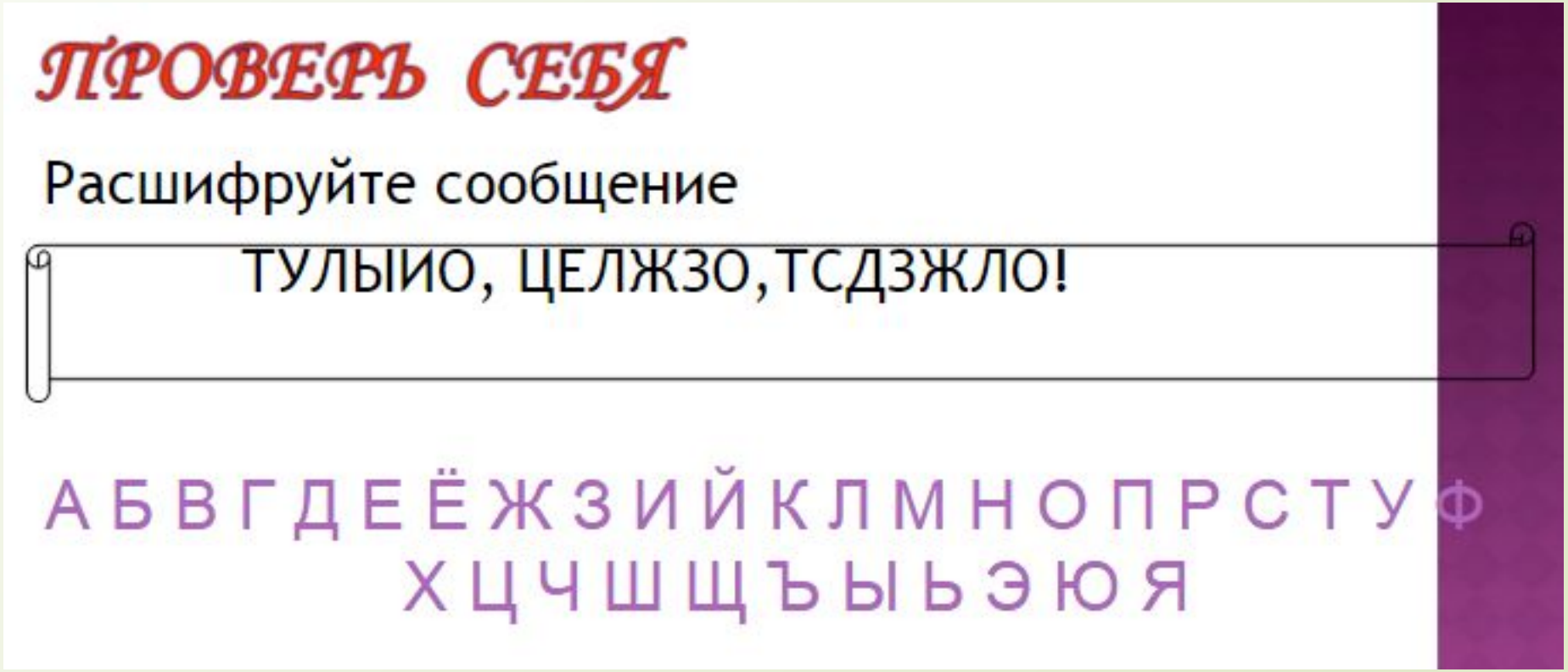
Заключается в замене букв открытого текста (верхней строки) на буквы (нижней строки) в соответствии с таблицей:

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
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

Например, слово CAESAR шифровалось бы как:

FDHVDU

Шифр Цезаря


ПРОВЕРЬ СЕБЯ
Расшифруйте сообщение
ТУЛЫИО, ЦЕЛЖЗО,ТСДЗЖЛО!
А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф
Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Шифр Цезаря

ПРОВЕРЬ СЕБЯ

Расшифруйте сообщение

ТУЛЫИО, ЦЕЛЖЗО,ТСДЗЖЛО!

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

Пришёл, увидел, победил!

Шифр равнозначной замены

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р
73	74	51	65	2	68	59	1	60	52	75	61	8	66	58	3

с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
69	64	53	54	9	62	71	4	67	56	72	63	55	70	57

Если шифрованное сообщение написано без пробелов между символами, то появляется дополнительная трудность при разбиении шифрованного сообщения на отдельные символы и слова.

Шифр равнозначной замены

Рассмотрим шифр простой замены, соответствующий таблице:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
11	98	33	42	19	13	87	54	43	49	48	50	69	32	73	18	81	29	76	74	22	31	90	59	67	77	91	12	52	45

Расшифруйте сообщение
733298131911

Пример шифров замены

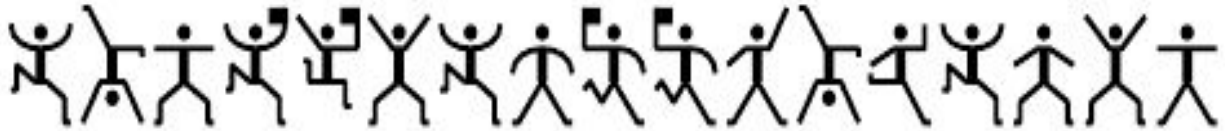
- Ж. Верн «Путешествие к центру Земли»

Пример шифров замены

А. Конан Дойл, «Пляшущие человечки»

В этом рассказе Холмсу необходимо было прочитать тексты пяти записок:

I. 

II. 

III. 

IV. 

V. 

Анализ шифров простой замены

Таблица 1 Частотность букв русского языка

i	Символ	*P(i)*	*i*	Символ	*P(i)*	*i*	Символ	*P(i)*
1	–	0,175	12	Л	0,035	23	Б	0,014
2	О	0,090	13	К	0,028	24	Г	0,012
3	Е	0,072	14	М	0,026	25	Ч	0,012
4	Ё	0,072	15	Д	0,025	26	Й	0,010
5	А	0,062	16	П	0,023	27	Х	0,009
6	И	0,062	17	У	0,021	28	Ж	0,007
7	Т	0,053	18	Я	0,018	29	Ю	0,006
8	Н	0,053	19	Ы	0,016	30	Ш	0,006
9	С	0,045	20	З	0,016	31	Ц	0,004
10	Р	0,040	21	Ь	0,014	32	Щ	0,003
11	В	0,038	22	Ъ	0,014	33	Э	0,003
						34	Ф	0,002

Анализ шифров простой замены

Шифры перестановки

Шифр, преобразования которого изменяют только порядок следования символов исходного текста, но не изменяют их самих, называется *шифром перестановки*.

Понятие шифра перестановки

Таблица шифра перестановки для текста длины n:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

где i_1 - номер места шифртекста, на которое перемещается первая буква исходного сообщения при выбранном преобразовании, i_2 - номер места для второй буквы и т. д.

Простой шифр перестановки

Расположим числа от 1 до 5 в двухстрочной записи, в которой вторая строка – произвольная перестановка чисел верхней строки:

12345

32514

Эта конструкция носит название подстановки,

а число 5 называется ее степенью.

Зашифруем фразу «СВЯЩЕННАЯ РИМСКАЯ ИМПЕРИЯ».

В этой фразе 23 буквы. Дополним её двумя произвольными буквами (например, Ь, Э) до ближайшего числа, кратного 5, то есть 25. Выпишем эту дополненную фразу без пропусков, одновременно разбив её на пятизначные группы:

СВЯЩЕ ННАЯР ИМСКА ЯИМПЕ РИЯЬЭ

Буквы каждой группы переставим в соответствии с указанной двухстрочной записью по следующему правилу: первая буква встаёт на третье место, вторая – на второе, третья – на пятое, четвёртая – на первое и пятая – на четвёртое. Полученный текст выписывается без пропусков:

ЩВСЕЯЯННРАКМИАСПИЯЕМЬИРЭЯ

При расшифровании текст разбивается на группы по 5 букв и буквы переставляются в обратном порядке: 1 на 4 место, 2 на 2, 3 на 1, 4 на 5 и 5 на 3. Ключом шифра является выбранное число 5 и порядок расположения чисел в нижнем ряду двухстрочной записи.

Шифр маршрутной перестановки

Зашифруем, например, фразу:

ПРИМЕРМАРШРУТНОЙПЕРЕСТАНОВКИ

используя прямоугольник размера 4×7:

П	Р	И	М	Е	Р	М
Н	Т	У	Р	Ш	Р	А
О	Й	П	Е	Р	Е	С
И	К	В	О	Н	А	Т

Зашифрованная фраза выглядит так:

МАСТАЕРРЕШРНОЕРМИУПВКЙТРПНОИ

Шифр вертикальной перестановки

Выписываются буквы по вертикали, а столбцы при этом берутся в порядке, определяемом ключом. Пусть, например, этот ключ таков: (5,4,1,7,2,6,3), и с его помощью надо зашифровать сообщение:

ВОТПРИМЕРШИФРАВЕРТИКАЛЬНОЙПЕРЕСТАНОВКИ

Впишем сообщение в прямоугольник, столбцы которого пронумерованы в соответствии с ключом:

5	1	4	7	2	6	3
В	О	Т	П	Р	И	М
Е	Р	Ш	И	Ф	Р	А
В	Е	Р	Т	И	К	А
Л	Ь	Н	О	Й	П	Е
Р	Е	С	Т	А	Н	О
В	К	И	–	–	–	–

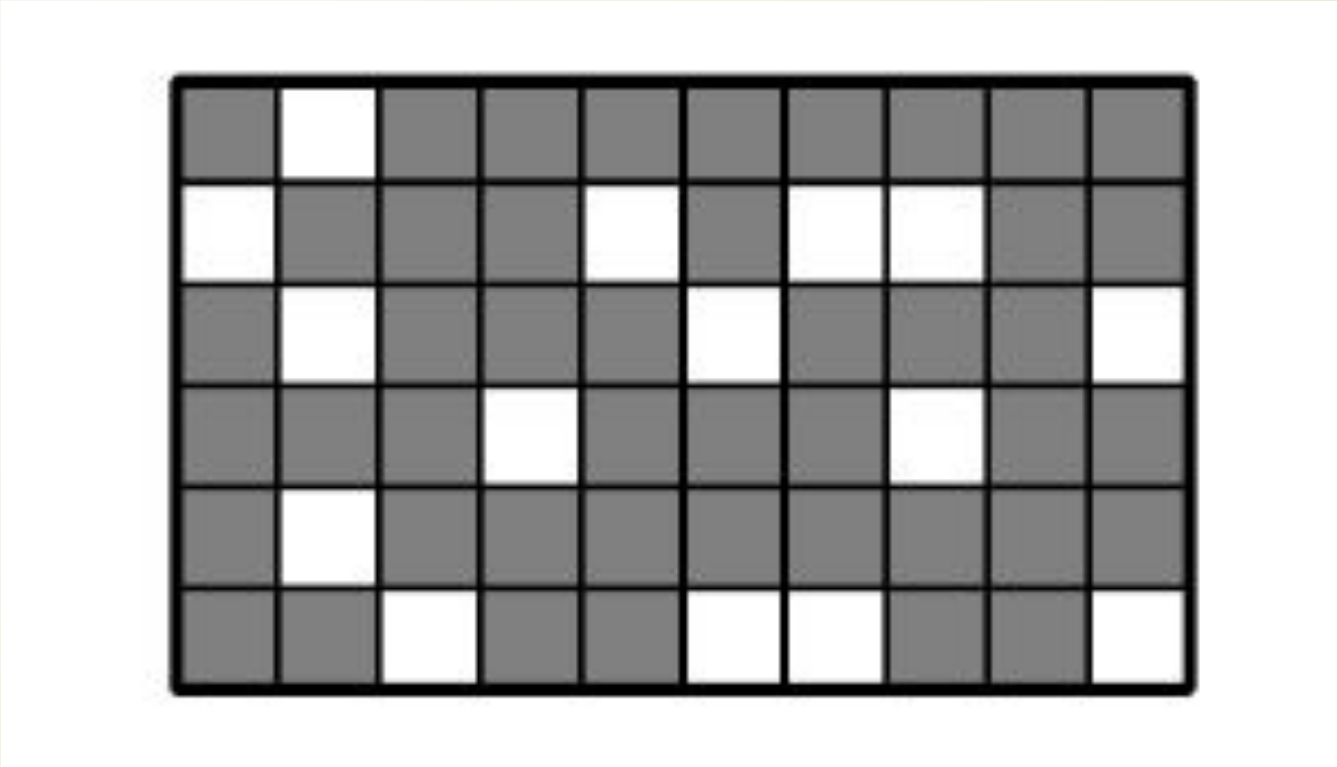
Теперь, выбирая столбцы в порядке, заданном ключом, и выписывая последовательно буквы каждого из них сверху вниз, получаем такую криптограмму:

ОРЕЬЕКРФИЙА–МААЕО–ТШРНСИВЕВЛРВИРКПН–ПИТОТ–

Шифр вертикальной перестановки

П	Е	Р	Е	С	Т	А	Н	О	В	К	А
9	4	10	5	11	12	1	7	8	3	6	2

Шифр поворотная решетка



Шифр поворотная решетка

ШИФРРЕШЕТКАЯВЛЯЕТСЯЧАСТНЫМСЛУЧАЕМШИФРАМАРШРУТНОЙПЕРЕСТАНОВКИ

	ь								
х				т		п	п		
	е				ь				е
			р				й		
	ю								
		ъ			б	к			ъ

Рис. 2

е	ь		р	я			ъ		
х				т		п	п	в	
	е	ю			ь	я			е
р			р	м			й	ш	
	ю	л	я		к				с
		ъ			б	к		в	ъ

Рис. 3

е	ь	ю	р	я	е	л	ъ		ь
х	х			т		п	п	в	
	е	ю	т		ь	я	п		е
р	ю		р	м	л		й	ш	ю
п	ю	л	я	ь	к	п	с		с
	р	ъ			б	к		в	ъ

Рис. 4

е	ь	ю	р	я	е	л	ъ	м	ь
х	х	н	и	т	о	п	п	в	е
п	е	ю	т	е	ь	я	п	я	е
р	ю	р	р	м	л	ю	й	ш	ю
п	ю	л	я	ь	к	п	с	м	с
н	р	ъ	б	й	б	к	х	в	ъ

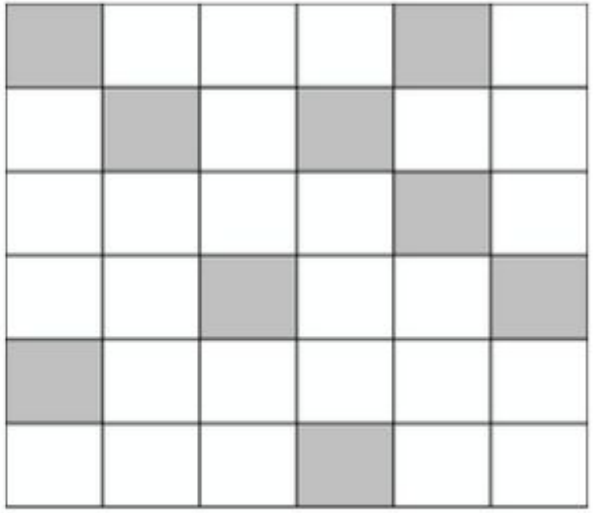
Рис. 5

Шифр поворотная решетка

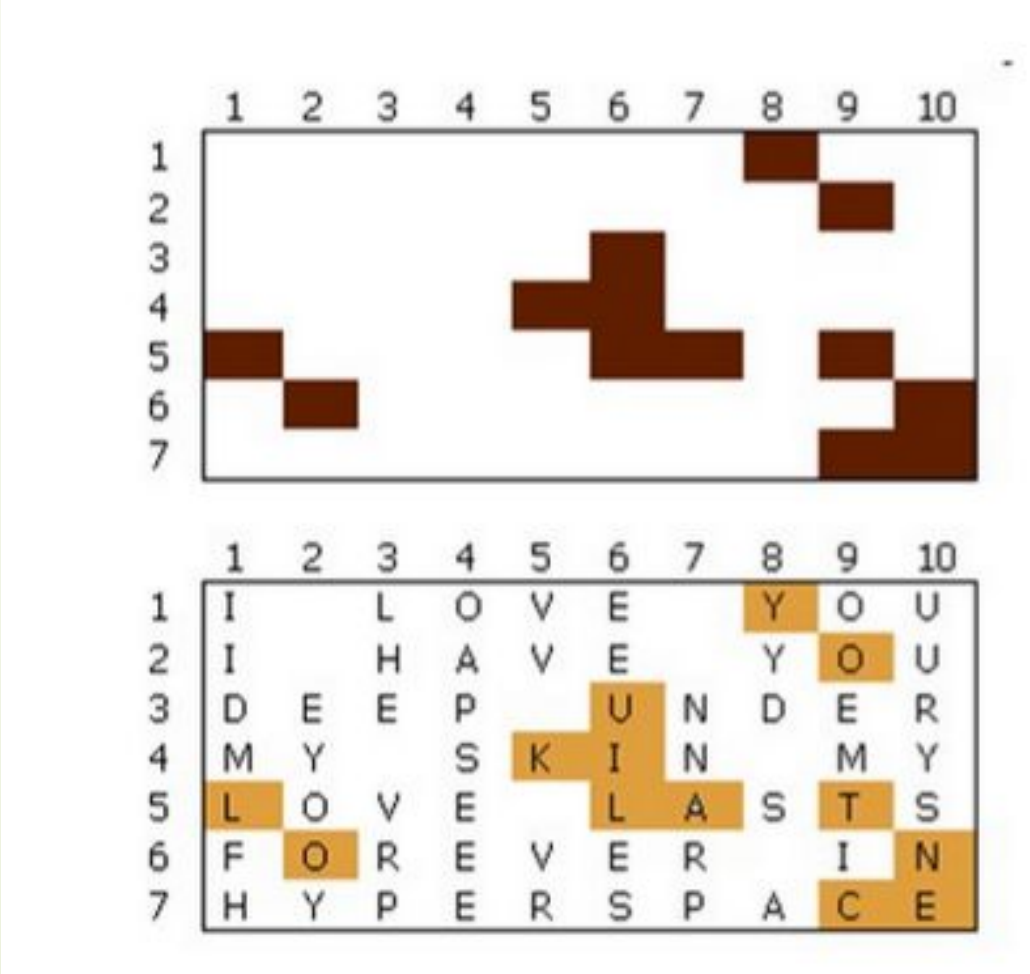
ПРОВЕРЬ СЕБЯ

Расшифруйте сообщение, используя одну из разновидностей решётки Кардано – поворотную решётку.

Э	Н	И	И	Т	Т
В	А	Н	Н	Е	П
Е	А	Р	Р	А	Я
Е	С	У		С	К
А		П	Н	Е	А
	К	Я	И		Т



Шифр Ришелье (объединение криптографии и стеганографии)



	1	2	3	4	5	6	7	8	9	10
1	I		L	O	V	E		Y	O	U
2	I		H	A	V	E		Y	O	U
3	D	E	E	P		U	N	D	E	R
4	M	Y		S	K	I	N		M	Y
5	L	O	V	E		L	A	S	T	S
6	F	O	R	E	V	E	R		I	N
7	H	Y	P	E	R	S	P	A	C	E

Шифры многозначной замены

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

то сообщение «я знаком с шифрами замены» может быть зашифровано, например, любым из следующих трех способов:

16 55 54 10 69 09 61 89 29 90 49 44 10 08 02 73 21 32 83 54 74

41 55 77 10 23 68 08 20 66 90 76 44 21 61 90 55 21 61 83 54 42

57 30 27 10 91 68 32 20 80 02 49 45 40 32 46 55 40 08 83 27 42

Упражнения

https://learningapps.org/460431

https://learningapps.org/2978300

https://learningapps.org/2752735