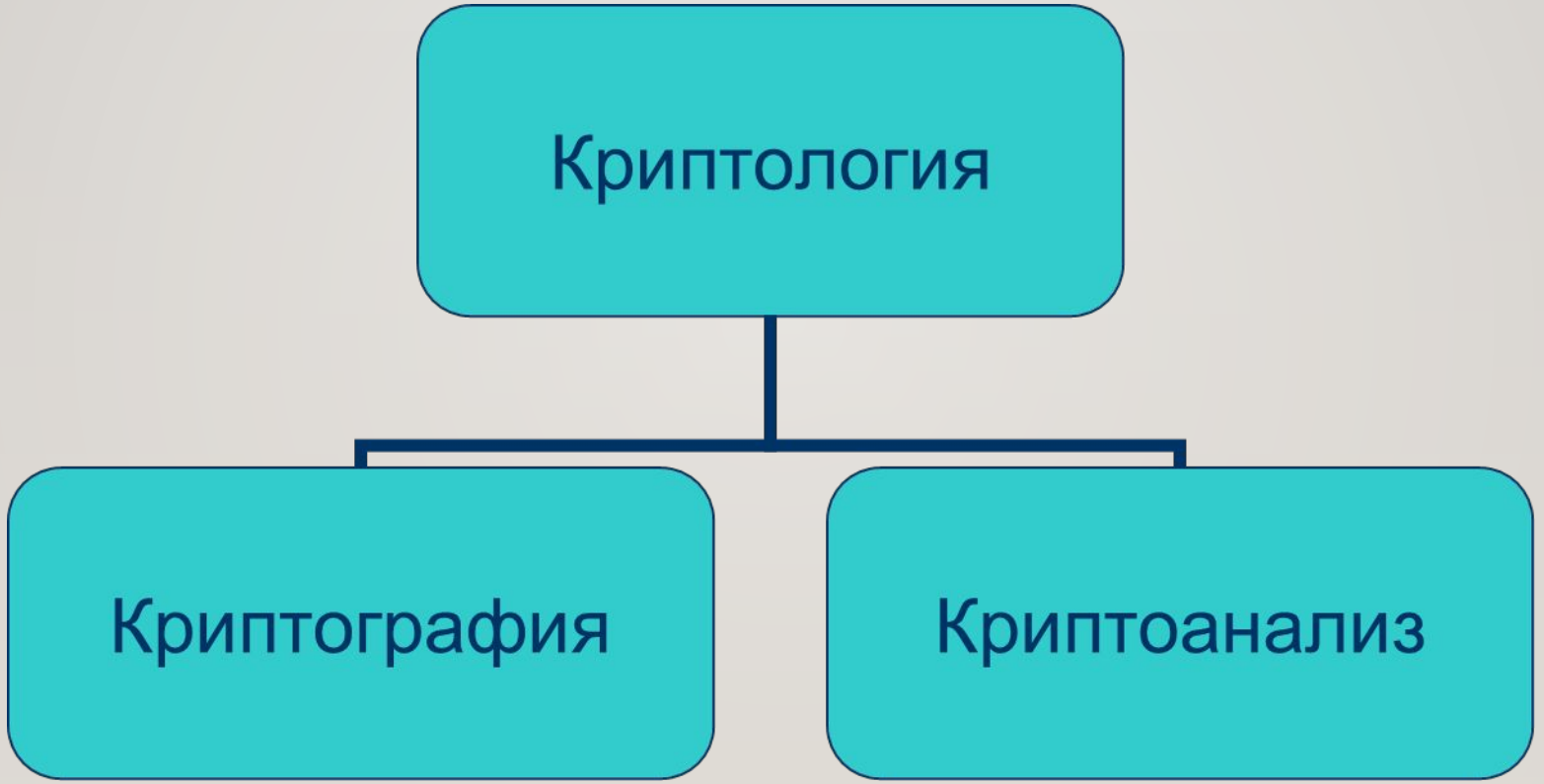
ЗАЧЕМ НУЖНА КРИПТОГРАФИЯ???

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.*

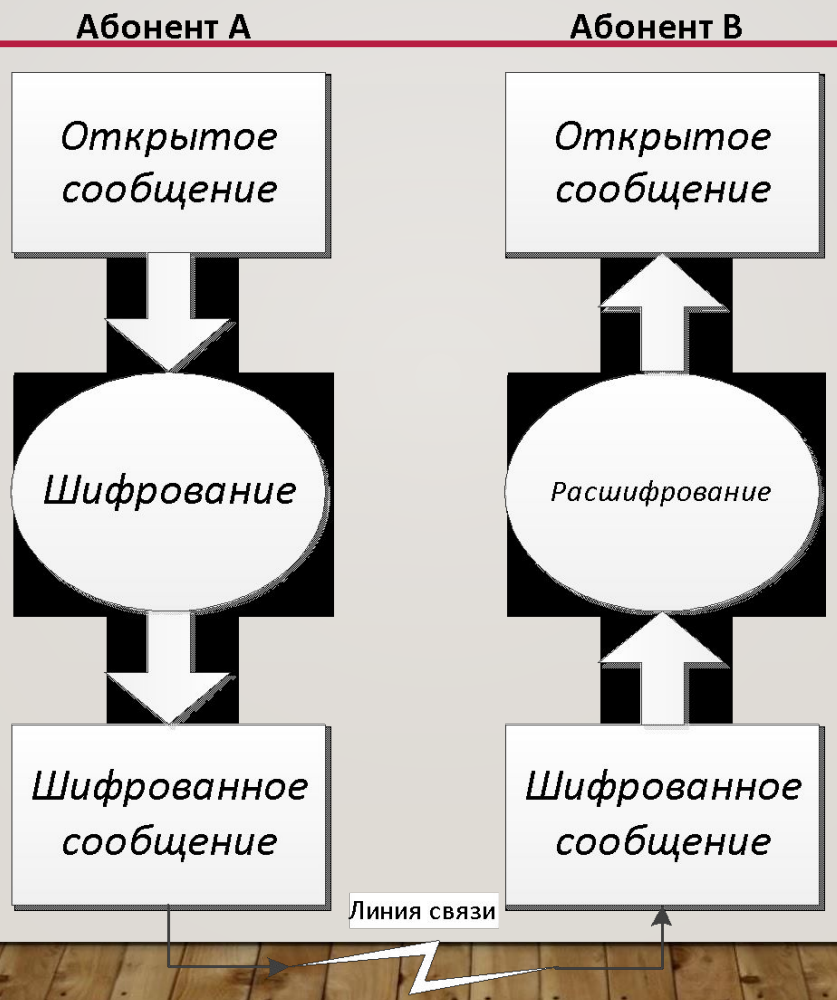

Криптология
Криптография
Криптоанализ

ЧТО ТАКОЕ КРИПТОГРАФИЯ???

Криптография («криптос» - тайна, «графэйн» - писать) - *наука о методах обеспечения*

- *конфиденциальности (невозможности прочтения информации посторонним)*
- *аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.*

ОСНОВНЫЕ ТЕРМИНЫ КРИПТОГРАФИИ



ПОНЯТИЕ ШИФРА

Обозначим буквой

- X - открытое сообщение,
- Y - шифрованное сообщение,
- f - правило шифрования,
- g - правило расшифрования.

Тогда зашифрование X в Y можно записать в виде

$$f(X) = Y.$$

Обратное преобразование (то есть получение открытого сообщения X путем расшифрования Y) запишется в виде соотношения

$$g(Y) = X.$$

ПРОЦЕСС ЗАШИФРОВАНИЯ

Используя понятие *ключа*, процесс зашифрования можно описать в виде соотношения:

$$f_k(X) = Y,$$

в котором k - выбранный ключ, известный отправителю и адресату.

Обратное шифрпреобразование в таком случае запишется так:

$$g_k(Y) = X.$$

Традиционна следующая терминология:

Дешифрование - преобразование шифртекста в открытый текст без использования секретного ключа.

- **Расшифрование** осуществляет лицо, знающее секретный ключ – адресат сообщения;
- **Дешифование** осуществляет лицо, не знающее секретного ключа - нарушитель.

ПРОСТЕЙШИЕ ШИФРЫ

Шифры

замены

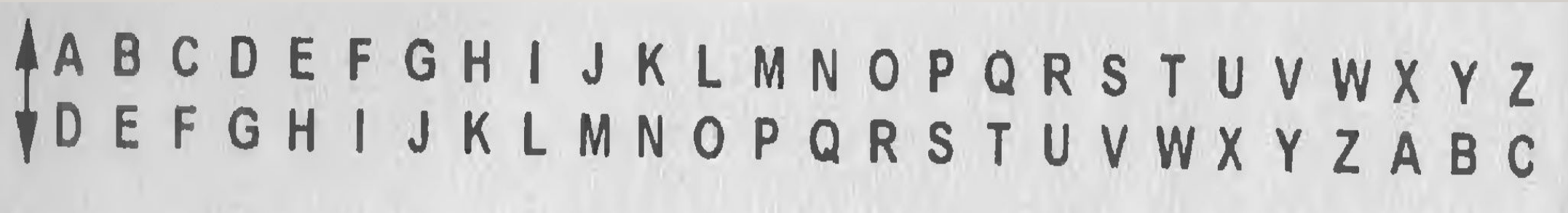
перестановки

ПРОСТЕЙШИЕ ШИФРЫ

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

СДВИГОВЫЕ ШИФРЫ

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



Например, слово CAESAR шифровалось бы как:

FDHVDU

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

В этом случае, например слово «ПОБЕДА» перейдет в

73 32 98 13 19 11

ШИФР ПРОСТОЙ ЗАМЕНЫ

Таблицы замены

А	*	Е
Б	/	Ф
В	+	О
Г	-	Ь
Д	%	З
Е	«	Р
Ё	«	Я
Ж	»	Г
З	!	Ц
И	?	Ш
Й	№	М

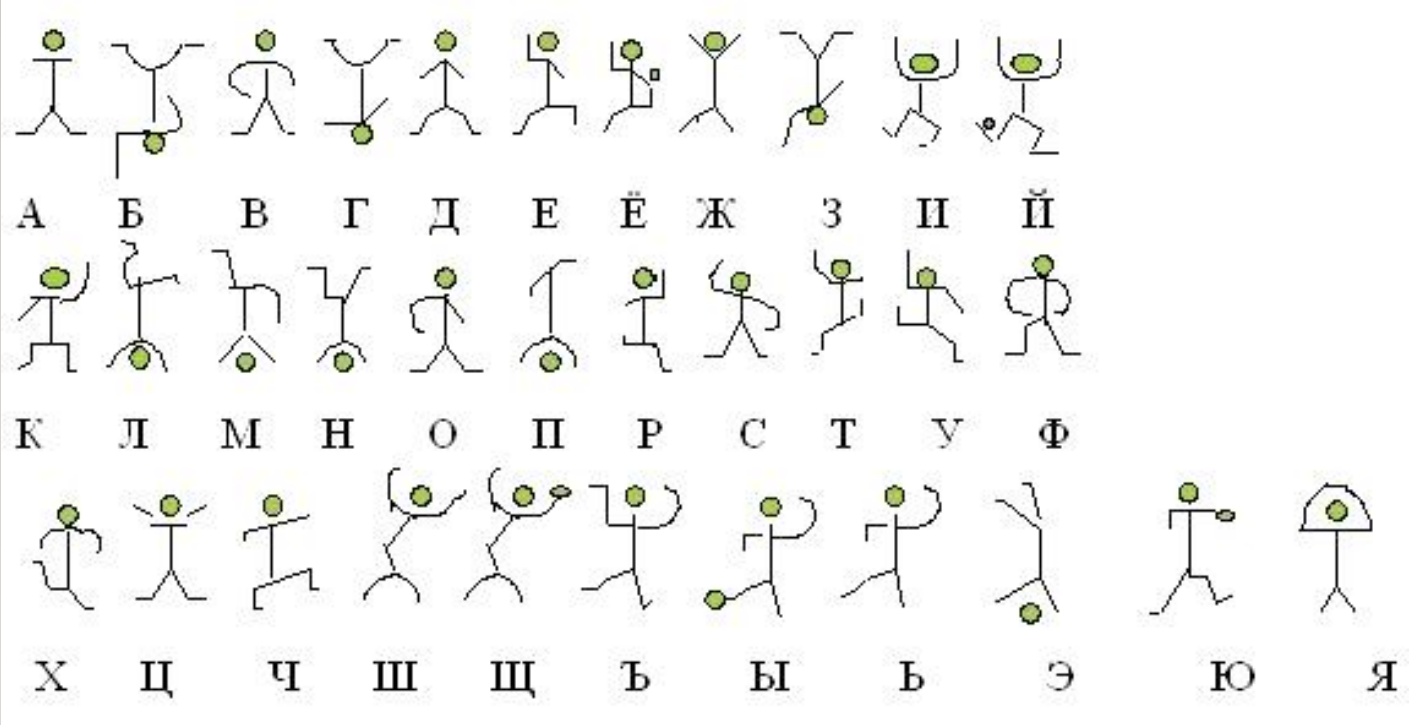
К	(	В
Л	)	Х
М	[	Н
Н	]	И
О	{	Ч
П	}	Ъ
Р	:	А
С	^	Щ
Т	;	К
У	$	Ж
Ф	№	Т

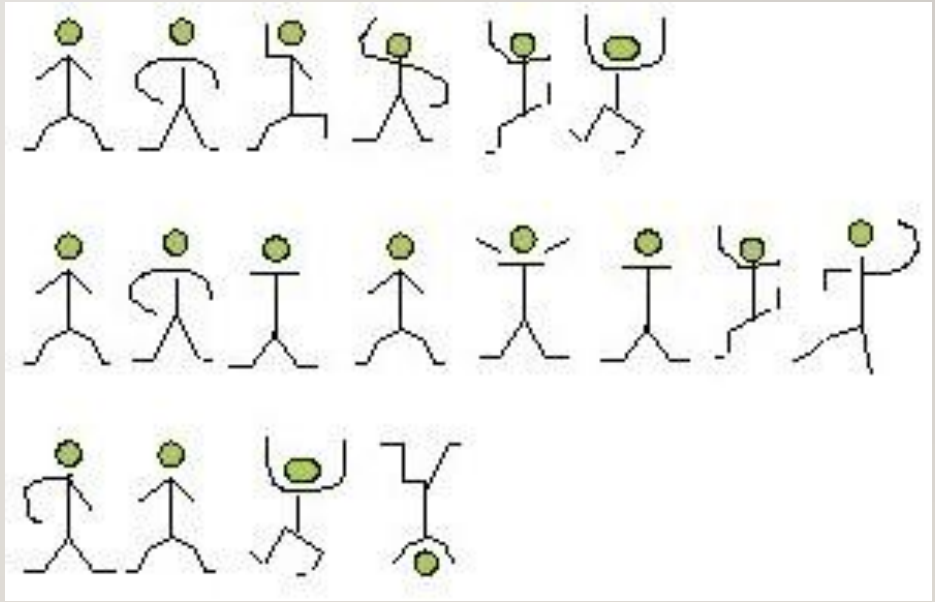
Х	=	Ё
Ц	&	С
Ч	\	Л
Ш	|	Б
Щ	@	Ы
Ъ	<	Ю
Ы	>	Й
Ь	.	Э
Э	`	У
Ю	~	П
Я	_	Д

Пример тайной переписки

}:?[«: ;*№]{№ }«:«}?^(?

ШИФР «ПЛЯШУЩИЕ ЧЕЛОВЕЧКИ»





АКРОСТИХ — ОСМЫСЛЕННЫЙ ТЕКСТ (СЛОВО, СЛОВОСОЧЕТАНИЕ ИЛИ ПРЕДЛОЖЕНИЕ), СЛОЖЕННЫЙ ИЗ НАЧАЛЬНЫХ БУКВ КАЖДОЙ СТРОКИ СТИХОТВОРЕНИЯ.

- **Д**овольно именем известна я своим;
  Равно клянётся плут и непорочный им,
  Утехой в бедствиях всего бываю боле,
  Жизнь сладостней при мне и в самой лучшей доле.
  Блаженству чистых душ могу служить одна,
  А меж злодеями — не быть я создана.

ЛИТОРЕЯ

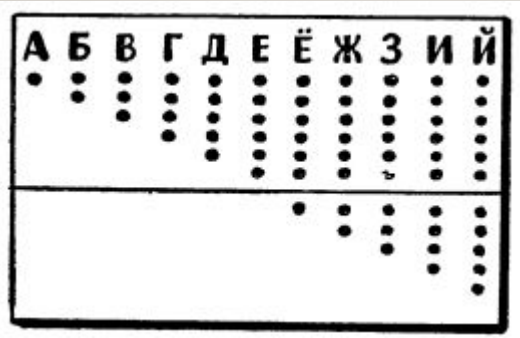
Литорея — род шифрованного письма, употреблявшегося в древнерусской рукописной литературе. Бывает простая и мудрая. Простую называют тарабарской грамотой, она заключается в следующем: поставив согласные буквы в два ряда в порядке:

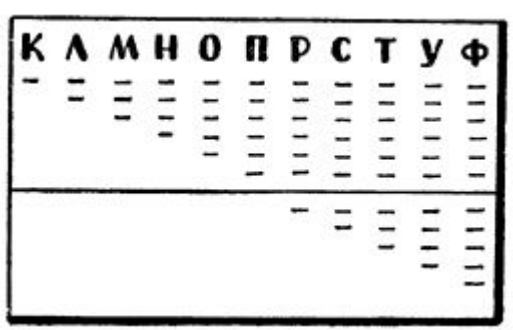
б	в	г	д	ж	з	к	л	м	н
щ	ш	ч	ц	х	ф	т	с	р	п

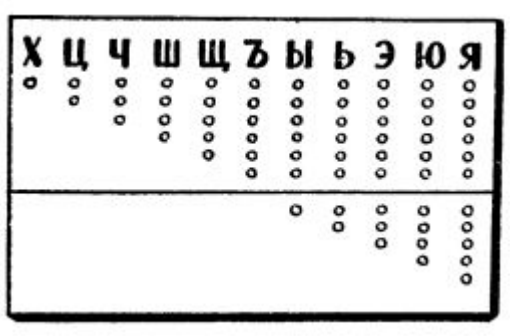
употребляют в письме верхние буквы вместо нижних и наоборот, причём гласные остаются без перемены;
Например, **токепот = котёнок**
Сикомея? Дефамь? Визмокетлк?

МУДРАЯ ЛИТОРЕЯ

- Весь алфавит разбивался на три группы, по десяти букв в каждой. Первый десяток букв обозначался точками. Например, «а» – одна точка, «б» – две точки и так далее.Второй десяток обозначался черточками. Например: «л» – одна черточка, «м» – две черточки и так далее. И, наконец, третий десяток обозначался кружками. Например, «х» – один кружок, «ц» – два кружка…

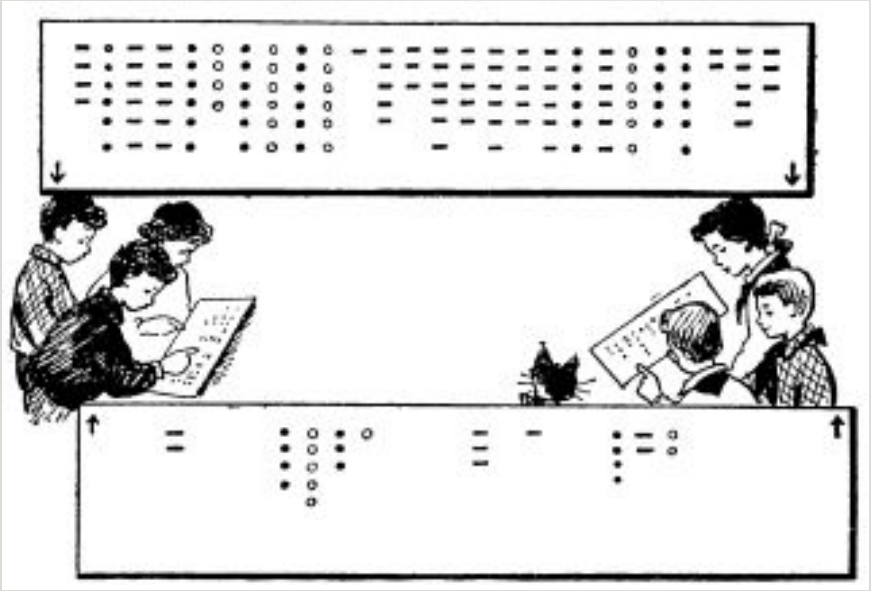




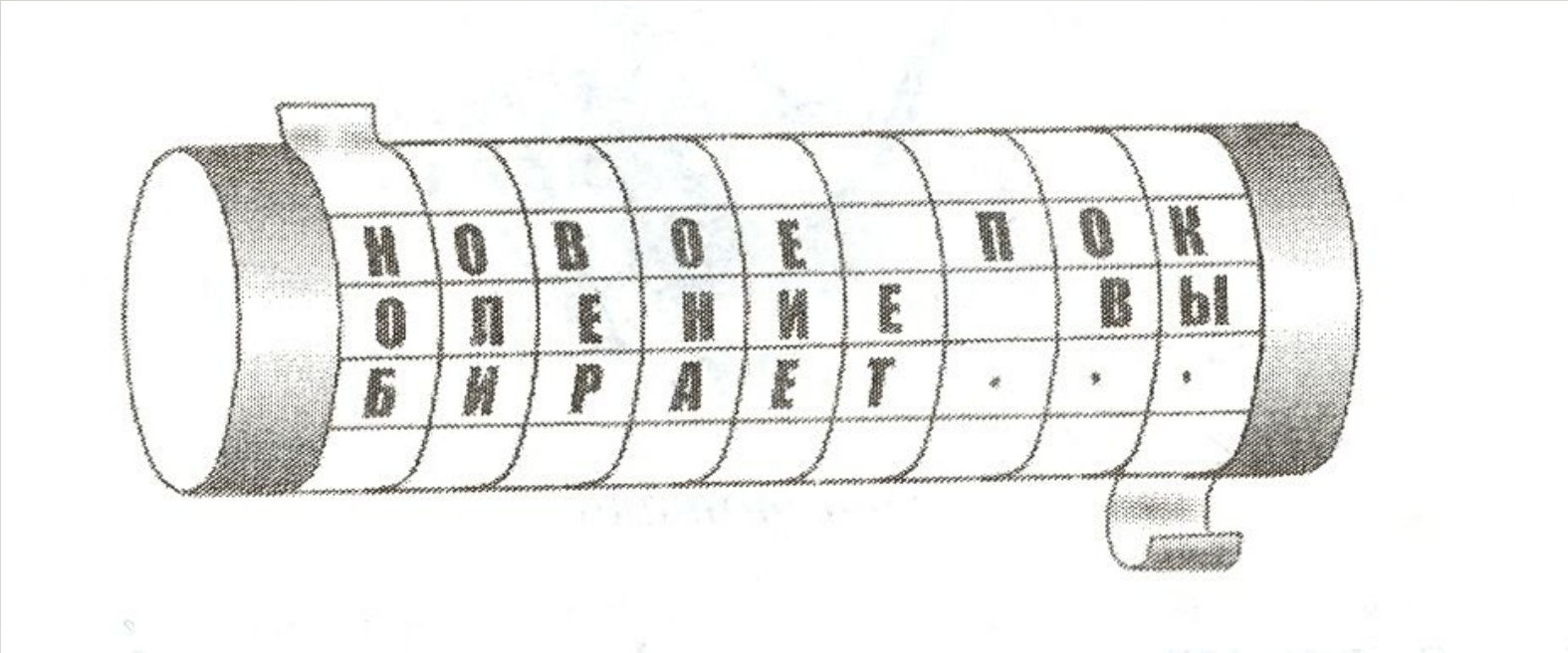


МУДРАЯ ЛИТОРЕЯ

Текст, зашифрованный таким способом, разделяли по горизонтали на две равные части, которые надлежало хранить порознь. Расшифровать написанное мудрой литореей можно было, только имея обе половинки текста.



ШИФР СЦИТАЛО



Ключом данного шифра являлся диаметр палки (сциталы).

КВАДРАТ ПОЛИБИЯ (СИГНАЛЬНЫЙ ШИФР)

Квадрат Полибия					
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z