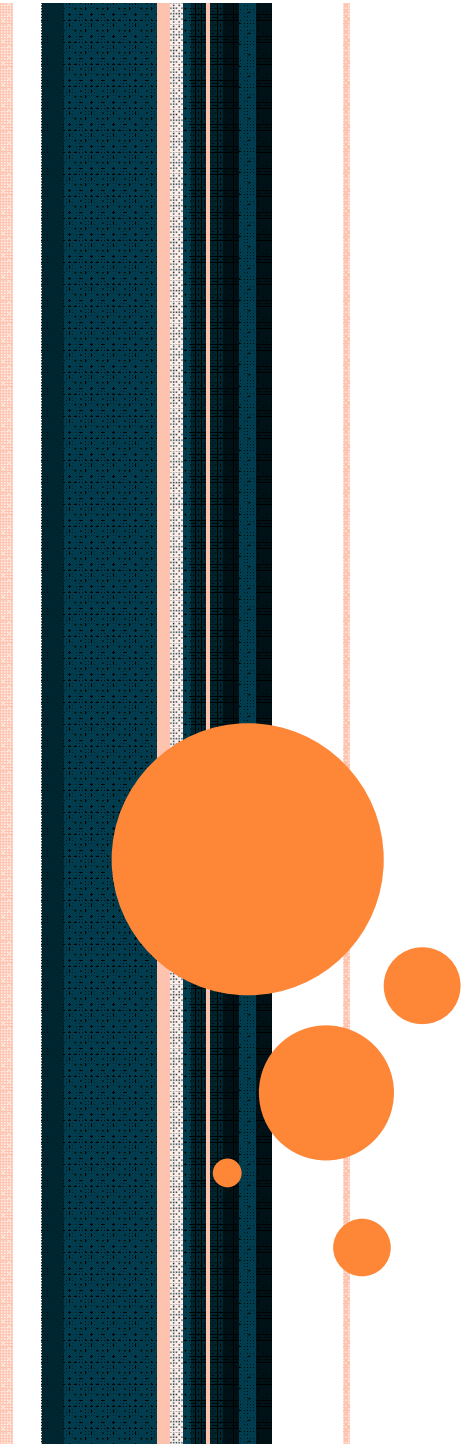


A decorative vertical bar on the left side of the slide. It consists of a thick dark teal bar with a fine grid pattern, flanked by thin orange lines. To the right of the teal bar are five orange circles of varying sizes, arranged in a descending staircase pattern.

КРИПТОГРАФИЯ. КРИПТОАНАЛИЗ

ШИФРЫ ЗАМЕНЫ

А	Б	...	Я
М _А	М _Б	...	М _Я

Таблица шифрозамен



ШИФРЫ ЗАМЕНЫ

ШИФР ЦЕЗАРЯ

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

- Ключ – сдвиг (количество позиций сдвига)
- Задача. Определите ключ для данного шифра Цезаря
- Задача. Зашифруйте слово **ИНФОРМАТИКА**



ШИФРЫ ЗАМЕНЫ

АТБАШ

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	Ы	Ь	Ъ	Э	Ю	Я

- Задача. Зашифруйте слово **ИНФОРМАТИКА**



ШИФРЫ ЗАМЕНЫ

ПОЛИБИАНСКИЙ КВАДРАТ

	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	Ъ	Ы	Ь
6	Э	Ю	Я	-	-	-

- Задача. Зашифруйте слово **ИНФОРМАТИКА**



ШИФРЫ ЗАМЕНЫ

ШИФРУЮЩАЯ СИСТЕМА ТРИТЕМИЯ

- Ключ – слово
- Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца.
- Задача. Зашифруйте слово **ИНФОРМАТИКА**

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

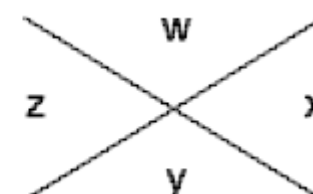
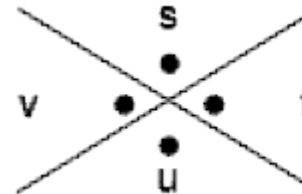


ШИФРЫ ЗАМЕНЫ

ШИФР МАСОНОВ

c	•	•	f	•	i
b	•	•	e	•	h
a	•	•	d	•	g

l	o	r
k	n	q
j	m	p



- Задача. Зашифруйте слово **INFORMATIQUE**
- Задача. Расшифруйте



ШИФРЫ ЗАМЕНЫ

ДИСК АЛЬБЕРТИ



ШИФРЫ ЗАМЕНЫ

ТАБЛИЦА ТРИСЕМУСА

- Первая буква текста шифруется по первой строке, вторая буква по второй и так далее. После использования последней строки вновь возвращаются к первой.
- Задача. Зашифруйте слово **ИНФОРМАТИКА**

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



ШИФРЫ ЗАМЕНЫ

ШИФР ВИЖЕНЕРА

[illegible]

- Ключ - слово
- Задача. Зашифруйте слово **ИНФОРМАТИКА**



ШИФРЫ ПЕРЕСТАНОВКИ

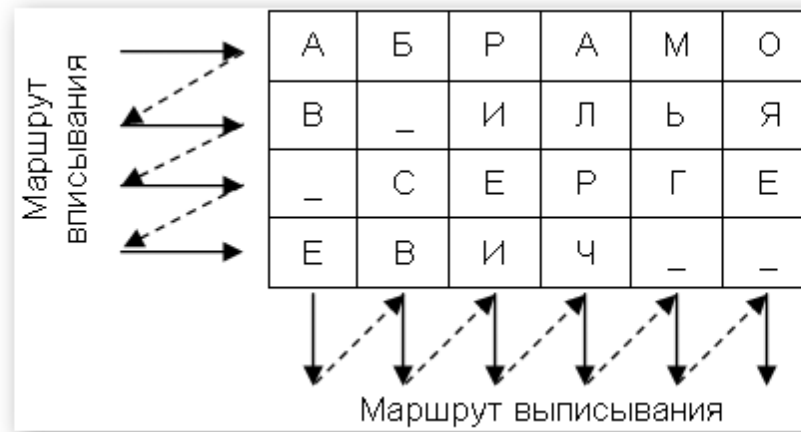
ШИФР ПРОСТОЙ ПЕРЕСТАНОВКИ

1	2	3	...	n
l_1	l_2	l_3	...	l_n



ШИФРЫ ЗАМЕНЫ

ШИФР МАРШРУТНОЙ ПЕРЕСТАНОВКИ



- Ключ – размер таблицы
- Задача. Определите ключ для данного шифра
- Задача. Ключ 3x4. Зашифруйте слово **ИНФОРМАТИКА**



ШИФРОВАНИЕ С ОТКРЫТЫМ КЛЮЧОМ

Шифр RSA

○ Процедура создания ключей

№ п/п	Описание операции	Пример
1	Выбираются два простых числа ¹ p и q .	$p=7, q=13$
2	Вычисляется произведение $n = p * q$.	$n=91$
3	Вычисляется функция Эйлера ² $\varphi(n)$.	$\varphi(n) = (7-1)(13-1) = 91-7-13+1 = 72$
4	Выбирается открытый ключ e , как произвольное число ($0 < e < n$), взаимно простое ³ с результатом функции Эйлера ($e \perp \varphi(n)$).	$e=5$
5	Вычисляется закрытый ключ d , как обратное число ⁴ k e по модулю $\varphi(n)$, из соотношения $(d * e) \bmod \varphi(n) = 1$.	$(d * 5) \bmod 72 = 1, d = 29$
6	Публикуются открытый ключ (e, n) в специальном хранилище, где исключается возможность его подмены (общедоступном сертифицированном справочнике).	

1) **Простое число** — натуральное число, большее единицы и не имеющее других натуральных делителей, кроме самого себя и единицы.

2) Результат расчета **функции Эйлера** $\varphi(n)$ равен количеству положительных чисел, не превосходящих n и взаимно простым с n

3) **Взаимно простые числа** — числа, не имеющие общих делителей, кроме 1, т.е. наибольший общий делитель которых равен 1.

4) **Обратными числами по модулю m** называются такие числа n и n^{-1} , для которых справедливо выражение $(n * n^{-1}) \bmod m = 1$.

В безмодульной математике **обратное число** n^{-1} (обратное значение, обратная величина) - число, на которое надо умножить данное число n , чтобы получить единицу ($n * n^{-1} = 1$). Пара чисел, произведение которых равно единице, называются **взаимно обратными**. Например: 5 и $1/5$, $-6/7$ и $-7/6$.

ШИФРОВАНИЕ С ОТКРЫТЫМ КЛЮЧОМ

Шифр RSA

- Процедуры шифрования и дешифрования выполняются по следующим формулам

$$C = T^e \bmod n$$

$$T = C^d \bmod n$$

- Пример шифрования (коды букв соответствуют их положению в русском алфавите, начиная с 1)

Открытое сообщение, T	Символ	А	Б	Р	А	М	О	В
	Код	1	2	18	1	14	16	3
Шифрограмма, $C = T^5 \bmod 91$		1	32	44	1	14	74	61
Открытое сообщение, $T = C^{29} \bmod 91$		1	2	18	1	14	16	3